UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN CIVIL LIBERTIES UNION, et al., Plaintiffs, v. ALBERTO R. GONZALES, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES, Defendant.	Civ. Act. No. 98-CV-5591

PLAINTIFFS' POST-TRIAL PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

Christopher A. Hansen
Aden Fine
Benjamin Wizner
Catherine Crump
American Civil Liberties Union
125 Broad Street – 18th Floor
New York, NY 10004
(212) 549-2693

Attorneys For Plaintiffs

Christopher Harris
Seth Friedman
Katharine Marshall
Jeroen Van Kwawegan
Latham & Watkins LLP
885 Third Avenue
New York, NY 10022
(212) 906-1800

Attorneys For Plaintiffs

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN CIVIL LIBERTIES UNION, et al. Plaintiffs, v. ALBERTO R. GONZALES, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES Defendant.	Civil Action No. 98-CV-5591

PLAINTIFFS' POST-TRIAL PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

I. COPA CHILLS A SUBSTANTIAL AMOUNT OF PROTECTED SPEECH.

A. Plaintiffs and Others Reasonably Believe COPA Proscribes Their Speech.

1. Plaintiffs and Others Reasonably Believe Their Speech Qualifies as "Harmful to Minors."

1. There are numerous examples of material on Plaintiffs' Web pages that contain an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast that might be considered harmful to minors. Walsh Testimony, Oct. 23 Transcript, at 141:10-17, 144:3-145:8, 146:6-13, 146:24-147:5, 147:9-18, 147:25-148:12, 152:8-15; Griscom Testimony, Oct. 23 Transcript, at 68:16-69:1, 70:4-9, 73:25-74:6, 74:16-23, 77:10-14, 79:7-13; P. Exh. 39, at 1-5, 61-63, 75-78, 64-74, 94-100, 101-111, 119-135; Glickman Testimony, Oct. 30 Transcript, at 130:23-131:10; P. Exh. 40;

Peckham Testimony, Oct. 31 Transcript, at 27:3-4; Corinna Testimony, Nov. 2 Transcript, at 81:10-15, 82:7-12, 87:25-88:6, 89:6-11, 95:10-15.

2. Nerve is an online magazine "about sex and culture." Griscom Testimony, Oct. 23 Transcript, at 52:13-4; Joint Exhibit ("J. Exh.") 1, ¶38.

3. Nerve has speech that "frequently" includes nudity and descriptions of sexual acts. Griscom Testimony, Oct. 23 Transcript, at 58:7-13, 66:18-79:13; 79:7-10; P. Exh. 38; J. Exh. 1, ¶39-40.

4. Nerve has video and blog sections that include nudity and depictions of sexual acts and sexual contact that are available for free and accessible to anyone. Griscom Testimony, Oct. 23 Transcript, at 73:24-74-6, 77:2-78:7.

5. Nerve has one million unique visitors per month. Griscom Testimony, Oct. 23 Transcript, at 54:25-55:3.

6. Salon is an online news organization devoted to news, politics, culture, arts, and life-style issues. Joan Walsh is the Editor-in-Chief of Salon. Walsh Testimony, Oct. 23 Transcript, at 90:14-18; J. Exh. 1, ¶ 25-26.

7. Salon was founded to offer an alternative to traditional newspapers and to create a hybrid kind of news organization that would combine news reporting and cultural commentary, and push the envelope on subjects and stories that other news organizations were not willing to cover. Walsh Testimony, Oct. 23 Transcript, at 110:12-112:1.

8. Salon's Web site, Salon.com, contains speech, both text and images, that describes and depicts sexual acts and sexual contact, including speech describing or depicting actual or simulated sexual acts or sexual contact, actual or simulated normal or

perverted sexual acts, and lewd exhibitions of the genitals or post-pubescent female breasts. Walsh Testimony, Oct. 23 Transcript, at 141:10-17, 144:3-145:8 (discussing article entitled "My Date With A Virtual Sex Machine"), 146:6-13, 146:24-147:5 (discussing sexually explicit Japanese wood cuts), 147:9-18 (discussing sex gallery photographs from Kinsey Institute, including one "depicting penetration of a man and a woman"), 147:25-148:12 (discussing Abu Ghraib photographs), 152:8-15 (discussing explicit photographs on a blog entitled "My So-Called Lesbian Life"); P. Exh. 39, at 1-5, 61-63, 75-78, 64-74, 94-100, 101-111, 119-135.

9. On average, about 3.1 million unique visitors access Salon's Web site on a monthly basis. That figure approximates the number of distinct individuals that visit the Web site. Walsh Testimony, Oct. 23 Transcript, at 116:1-4, 116:5-20.

10. Condomania is a specialty retailer, headquartered in California and incorporated in Massachusetts, that sells condoms, safer sex, and romance-related products through a physical store in New York City and through its website, www.condomania.com. Glickman Testimony, Oct. 30 Transcript, at 92:8-23, 94:12-95:1; J. Exh. 1, ¶8.

11. Adam Glickman is the founder, president, and CEO of Condomania. Glickman Testimony, Oct. 30 Transcript, at 91:11-92:5.

12. Condomania contains speech that depicts and describes human genitalia, sexual acts, and sexual contact. Glickman Testimony, Oct. 30 Transcript, at 130:23-131:10; Pl. Ex. 40.

13. The Sexual Health Network provides educational resources and information on subjects related to sexual health, primarily through its Web site, sexualhealth.com.

Dr. Mitchell Tepper is the founder and President of the Sexual Health Network. Tepper Testimony, Oct. 30 Transcript, at 174:1-15.

14. The Sexual Health Network's Web site contains frank and sexually explicit speech, including text and videos, that describes and depicts actual or simulated sexual acts or sexual contact, actual or simulated normal or perverted sexual acts, and lewd exhibitions of the genitals or post-pubescent female breasts. Tepper Testimony, Oct. 30 Transcript, at 205:10-15, 206:19-207:24 (discussing article entitled "The Joys That Vibrators Can Bring To Your Sex Life"), 208:14-209:6 (discussing content found within topic entitled "Keeping Sex Fun"), 209:15-210:15 (discussing article entitled "Spicing Up Your Sex Life"), 211:3-23 (discussing user question and expert answer about using a strap-on dildo to engage in anal penetration), 213:1-18 (discussing content in the section captioned "Sexuality Education"), 213:19-214:25 (discussing webcast videos on the site and a sexual fetish video), 215:5-13 (discussing sexual aid products shopping portion of site), 184:1-12 (discussing the videos on the site); P. Exh. 37, at 1-3, 4-7, 8-9, 10-13, 14-15, 16-17, 73, 74, 76, 77, 78, 79, 80-87, 90-92, 93-94, 95-99.

15. There are dozens of Web sites in addition to the Sexual Health Network's Web site that contain similar speech about sexual health and sexual education and provide frank and sexually explicit information. As with the Sexual Health Network's Web site, none of those sites requires users to provide personally identifiable information to access the material on those sites. Tepper Testimony, Oct. 30 Transcript, at 231:20-232:9.

16. Dr. Tepper has testified in several lawsuits challenging state legislation similar to COPA. In each instance, the Sexual Health Network's speech on the Web was

determined to be at risk under those state versions of COPA. Each of those courts also declared that the state laws were unconstitutional, and none of those state laws was permitted to be enforced. Tepper Testimony, Oct. 30 Transcript, at 203:14-204:4.

17. The Sexual Health Network's Web site receives 135,000-150,000 user sessions per month, which means that it receives approximately 135,000-150,000 visitors per month. Tepper Testimony, Oct. 30 Transcript, at 178:24-179:11.

18. Urbandictionary.com is an online dictionary with an emphasis on slang. All of its words and definitions are supplied by visitors to the site. Testimony of Aaron Peckham, Oct. 31 Transcript, at 22:4-9; J. Exh. 1, ¶18, 19.

19. There are approximately one million definitions on urbandictionary.com's website. Peckham testimony, Oct. 31 Transcript, 26:9-12. Eighteen of the 20 most frequently searched words on urbandicitonary.com are sexually explicit. *Id.* at 27:3-4. See also J. Exh. 1, ¶41, 42. Urbandictionary.com also includes sounds and images, including images that depict the genitals or the post-pubescent female breast. *Id.* at 44:1-12.)

20. Approximately 40 million people visited urbandictionary.com between January and October of 2006; 330,000 people visit the site on an average day. Peckham Testimony, Oct. 31 Transcript, 24:16-23. Urbandictionary.com has been ranked one of the top 1000 most visited sites on the Web. *Id.* at 24:9-15.

21. Approximately 37 percent of urbandictionary.com's users are from overseas, and approximately 10 percent are under 17. *Id.* at 25:14 to 26:8.

22. Scarletletters.com is a Web site "intended to deliver sexuality information as well as entertainment by women for female users." Corinna Testimony, Nov. 2 Transcript, 73:2-5; J. Exh. 1, ¶9-10, 35.

23. Scarletletters.com includes content that is sexually explicit. Corinna Testimony, Nov. 2 Transcript, 88:1-89:25; P. Exh. 42.

24. Scarletletters.com has about 2,000 visitors per day and has had as many as 6,000 per day. Corinna Testimony, Nov. 2 Transcript, 73:20-24.

25. Scarleteen.com is a "sex education and information clearing house that's aimed at teenagers and young adults." Corinna Testimony, Nov. 2 Transcript, 74:1-2; J. Exh. 1, ¶11, 34.

26. Scarleteen.com includes content that is sexually explicit. Corinna Testimony, Nov. 2 Transcript, 77:24-85:23; P. Exh. 42

27. Scarleteen.com has about 25,000 users per day. Corinna Testimony, Nov. 2 Transcript, 74:23-25.

28. Femmerotic.com provides sexuality information "by women pertaining to women." Corinna Testimony, Nov. 2 Transcript, 75:1-5; J. Exh. 1, ¶12, 36.

29. Femmerotic.com includes content that is sexually explicit. Corinna Testimony, Nov. 2 Transcript, 94:21-95:14, 127:13016; P. Exh. 42, pp. 17, 26-28.

30. Femmerotic.com has about 2,000 visitors per day. Corinna Testimony, Nov. 2 Transcript, 75:6-7.

31. Wayne Snellen is an artist and Director of the Leslie/Lohman Gay Art Foundation (the "Foundation"). Mr. Snellen is also Director of the Leslie/Lohman Gay Art Gallery (the "Gallery"), located in New York, New York and online at

www.leslie.lohman.org. Snellen Testimony, Nov. 2 Transcript, at 129:18-19, 130:24-131:18, 132:10-16.

32. Much of the art work on the Leslie Lohman Web site including Mr. Snellen's own work, is sexually explicit, depicts male genitalia, and depicts sexual acts, including sexual acts by same sex couples. Snellen Testimony, Nov. 2 Transcript, at 134:12-25, 143:24-150:5; P. Exh. 49.

33. There is a significant amount of art on the Internet similar to Mr. Snellen's art. Snellen Testimony, Nov. 2 Transcript, at 159:12-16.

34. Alicia Smith is a hip-hop musician who performs under the name God-Des. Her music is a combination of hip-hop, soul and rhythm and blues. Ms. Smith's goal as a musician is to be the first openly gay mainstream hip-hop artist. A. Smith Testimony, Oct. 26 Transcript, at 178:20-23, 182:6-9.

35. Ms. Smith's songs deal with classism, racism, homophobia, peer pressure for kids, and issues of sexuality. Her goal is to counter the negative images of women and violence in the hip-hop culture and to send out a message to gay people and women that it is okay to feel good about who they are. Ms. Smith's songs are also targeted to youth, especially gay and lesbian youth, who are struggling with their identity and might be having a difficult childhood because of their sexual orientation. A. Smith Testimony, Oct. 26 Transcript, at 182:10-25, 206:23-207:24, 218:4-14.

36. Ms. Smith's songs, particularly her song "Lick It," contain speech that describes human genitalia, post-pubescent female breasts, sexual acts, and sexual contact between two women that is frank, graphic, and explicit. A. Smith Testimony, Oct. 26

Transcript, at 183:11-12, 203:9-13, 204:11-15, 208:9-209:14; P. Exh. 50; P. Exh. 51; P. Exh. 83.

37. There are dozens of other gay and lesbian hip-hop musicians. All of them have songs that contain similar explicit, frank speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity. All of them make their songs available on the Web. A. Smith Testimony, Oct. 26 Transcript, at 191:14-192:9.

38. There are millions of other hip-hop musicians. The vast majority of them make their songs, many of which are sexually explicit, available on the Web. A. Smith Testimony, Oct. 26 Transcript, at 192:10-194:11.

39. Ms. Marilyn Jaye Lewis is the founder and Director of the Erotic Authors Association (EAA). The EAA's mission is to honor literary merit and achievement in the writing and publishing of erotic fiction. Lewis Testimony, Oct. 31 Transcript, at 81:21-82:05.

40. Ms. Lewis is herself an author of erotic fiction. She publishes both online and in traditional print media. Lewis Testimony, Oct. 31 Transcript, at 81:15-16, 82:06-86:12.

41. The EAA operates a Web site, which it uses to promote and sell the works of its members. Lewis Testimony, Oct. 31 Transcript, at 90:25-91:22.

42. Ms. Lewis' work and work by other authors can be found on the EAA Web site. The Web site contains speech that describes human genitalia, the post-pubescent female breast, sexual acts, and sexual contact that is frank and explicit. Lewis Testimony, Oct. 31 Transcript, at 96:04-108:25.

43. Ms. Lewis is aware of other Web sites that contain similar speech about human genitalia, the post-pubescent female breast, sexual contact and sexual activity that are frank and explicit. The EAA Website links to approximately 200 members' Web sites, where it is possible to view and purchase works containing similar speech. Lewis Testimony, Oct. 31 Transcript, at 89:07-22.

44. About 1,500 to 2,000 unique individuals visit the EAA Web site each day. Anyone can read any section of the EAA Web site without providing any information about themselves. There is no way to tell whether a particular visitor is a minor or an adult. Ms. Lewis is responsible for placement of material on the EAA Web site. Lewis Testimony, Oct. 31 Transcript, at 91:18-92:24, 93:11-94:05.

45. Barbara DeGenevieve is the chair of the Photography department at the School of the Art Institute of Chicago and an artist working in photography, video, and performance. DeGenevieve Testimony, Nov. 1 Transcript, at 4:18-6:16.

46. Professor DeGenevieve owns and operates the Web site www.degenevieve.com, which contains selections of her works from 1978 to the present as well as selections of her writings. DeGenevieve Testimony, Nov. 1 Transcript, at 24:21-27:4.

47. Any person with access to the World Wide Web may access www.degenevieve.com for free and without providing any personally identifying information or stating their age. DeGenevieve Testimony, Nov. 1 Transcript, at 27:5-15.

48. Professor DeGenevieve's Web site contains speech that depicts and describes human genitalia, the post-pubescent female breast, sexual acts, and sexual contact. DeGenevieve Testimony, Nov. 1 Transcript, at 28:17-55:22 ; P. Exh. 53.

49. Professor DeGenevieve is aware of other artists whose Web sites contain similarly sexually explicit speech. DeGenevieve Testimony, Nov. 1 Transcript, at 58:3-6.

50. Plaintiff American Civil Liberties Union ("ACLU") is a nationwide nonpartisan organization of over 400,000 members dedicated to defending the principles of liberty and equality in the Bill of Rights. J. Exh. 1, ¶ 4.

51. Patricia Nell Warren is a member of the American Civil Liberties Union. Ms. Warren is the author of numerous novels and other works, as well as the co-founder of Wildcat Press, which maintains a Web site that includes text and graphics. J. Exh. 1, ¶ 7.

52. Lawrence Ferlinghetti is a member of the American Civil Liberties Union. Mr. Ferlinghetti is the author of numerous novels and other works, as well as the co-founder of City Lights Bookstore and Publishing. City Lights maintains a Web site that features an extensive selection of books, in topics ranging from poetry and fiction to politics and music. J. Exh. 1, ¶ 5-6.

53. Members of the ACLU have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. For example, Patricia Nell Warren's Web site includes excerpts from her gay-themed literature, including sexually explicit details such as the description of a "foursome" erotically dancing and a description of two men passionately kissing. Members of the ACLU similarly access

speech on the Web that describes and depicts sexual acts and sexual contact that is frank and explicit. J. Exh. 1, ¶ 7.

54. Plaintiff Electronic Frontier Foundation ("EFF") is a nationwide nonprofit organization that is committed to defending civil liberties in the world of online computer communication. EFF members access speech on the Internet. J. Exh. 1, ¶ 13.

55. Members of EFF have Web sites that contain speech that describes and depicts sexual acts and sexual contact. Although those members believe their speech has value, even for older minors, they reasonably believe that many others do not share that view. J. Exh. 1, ¶ 13.

56. Plaintiff Electronic Privacy Information Center ("EPIC") is a non-profit research organization that collects and distributes information concerning civil liberties and privacy issues arising in the new communications media. EPIC contributors access speech on the Internet, including sexually explicit speech, as part of its mission. J. Exh. 1, ¶ 29, 46.

57. EPIC fears that if COPA were to go into effect the Web sites it reviews may remove from their Web sites materials similar to what which EPIC staff has heretofore been able to access without providing proof of age. EPIC does not intend to instruct its staff to use a credit card or adult access code to access Web sites. J. Exh. 1, ¶ 29, 46.

58. Plaintiff Powell's Bookstore is a reader-centered company that operates seven bookstores in Portland, Oregon, and maintains a Web site through which users can purchase new, used, rare, and out-of-print books. Powell's Bookstore is a longstanding member of the American Booksellers Foundation for Free Expression. J. Exh. 1, ¶ 22-24.

59. Plaintiff American Booksellers for Free Expression ("ABFFE") is a non-profit organization created to inform and educate booksellers, other members of the book industry, and the public about the dangers of censorship. ABFFE promotes and protects the free expression of ideas. J. Exh. 1, ¶22.

60. Members of ABFFE have Web sites that contain speech that describes and depicts sexual acts and sexual contact that is frank and explicit. J. Exh. 1, ¶ 45.

61. Plaintiff Free Speech Media, LLC, in partnership with Public Communicators, Inc., is a non-profit organization that operates freespeech.org. This Web site promotes independent audio and video content on the Web. J. Exh. 1, ¶ 15, 16.

62. Free Speech Media contains speech that describes and depicts sexual acts and sexual contact. Although it believes its speech has value, even for older minors, Free Speech Media reasonably believes that many others do not share that view. J. Exh. 1, ¶ 37.

63. Plaintiff Philadelphia Gay News is a for-profit corporation that has been the leading print and newspaper for the gay and lesbian community of Philadelphia since 1976. Philadelphia Gay News is also now published on the Web. J. Exh. 1, ¶ 20, 21.

64. Philadelphia Gay News reasonably fears prosecution under COPA. Its Web site contains speech that describes and depicts sexual acts and sexual contact. Its Web site addresses issues relevant to the gay and lesbian community. Philadelphia Gay News understands that some communities would consider access to personal advertisements inappropriate for minors when involving persons of the same gender, and that some communities may believe that its descriptions of social and sports clubs

catering to the gay and lesbian community to be harmful to minors because they "entice" young people into exploring gay life. J. Exh. 1, ¶ 43, 44.

2. Plaintiffs and Others Reasonably Believe COPA Proscribes User Generated Content on Their Web Pages.

65. Many of the Plaintiffs' Web sites have user-generated content, such as message boards, blogs, personals, and other interactive forums, that permit users to post text, images, and videos on the Web sites. Walsh Testimony, Oct. 23 Transcript, at 120:1-10; Tepper Testimony, Oct. 30 Transcript, at 182:17-20; Griscom Testimony, Oct. 23 Transcript, at 71:3-15; Peckham Testimony, Oct. 31 Transcript, at 22:7-9; Corinna Testimony, Nov. 2 Transcript, at 82:13-84:5.

66. Having user-generated content on their Web sites is an important part of Plaintiffs' sites because, among other things, it enables users who may have common interests or who are dealing with common issues to interact with each other and find out about issues affecting other people, and because user-generated content, such as the content on the YouTube.com Web site, is the fastest growing aspect of the Web, and one of the most popular, especially among minors. Walsh Testimony, Oct. 23 Transcript, at 120:11-23, 127:16-128:14; Tepper Testimony, Oct. 30 Transcript, at 189:19-25.

67. The user-generated aspects of Plaintiffs' sites generate a significant amount of traffic and help draw users to the Web sites, both to post their own material and to read what other users have posted. Walsh Testimony, Oct. 23 Transcript, at 120:122:6-17 (Salon receives hundreds of user letters per day and from 40,000 to 70,000 page views per day of these user letters), 133:14-17 (10-15 percent of Salon's total traffic stems from user-generated content).

68. Some of the user-generated content on Plaintiffs' Web sites depicts and describes sexual acts and sexual contact. Walsh Testimony, Oct. 23 Transcript, at 124:22-126:3 (discussing user letters generated in response to an article about bikini waxing), 152:3-15 (discussing a blog containing photographs of two women engaged in a sexual act); Tepper Testimony, Oct. 30 Transcript, at 186:12-187:5, 189:7-18, 187:17-19; P. Exh. 37; P. Exh. 39; Corinna Testimony, Nov. 2 Transcript, at 83:7-15, 84:4-5.

69. Plaintiffs publish this user-generated content knowing that their users may, and in fact do, place frank and explicit material that depicts and describes sexual acts and sexual contact on their Web sites. Walsh Testimony, Oct. 23 Transcript, at 124:22-25, 200:1-4; Tepper Testimony, Oct. 30 Transcript, at 187:17-19; Corinna Testimony, Nov. 2 Transcript, at 83:7-15, 84:4-5.

70. Most of the Plaintiffs do not pre-screen any of this user-generated content, so it is impossible for those Plaintiffs to prevent sexually explicit material from being accessible on their Web sites until after the material appears on the sites. Walsh Testimony, Oct. 23 Transcript, at 129:14-17.

71. Because most of the Plaintiffs do not pre-screen their user-generated content, the only way Plaintiffs could prevent minors from accessing user-generated content that is considered harmful to minors would be to place an age verification screen on the initial page of the user-generated content, before users could view any of the material. Walsh Testimony, Oct. 23 Transcript, at 129:8-13; Peckham Testimony, Oct. 31 Transcript, at 48:1-6.

72. Many of the Plaintiffs who publish user-generated content on their sites have employees or representatives who monitor, participate in, or help generate discussions

and content on the user-generated aspects of the sites. Walsh Testimony, Oct. 23 Transcript, at 126:24-127:15; Tepper Testimony, Oct. 30 Transcript, at 187:20-188:18; Corinna Testimony, Nov. 2 Transcript, at 82:18-83:6.

73. All of the Plaintiffs have editorial control over the content once it appears on the site and retain the right to delete or remove any user-generated content that they believe should not be on their site, for any reason. Walsh Testimony, Oct. 23 Transcript, at 124:1-125:5; Peckham Testimony, Oct. 31 Transcript, at 37:21-38:3. Appropriateness for minors or sexual explicitness is not one of the considerations that lead Plaintiffs to remove user-generated content. Walsh Testimony, Oct. 23 Transcript, at 119:23-24; Tepper Testimony, Oct. 30 Transcript, at 189:4-6.

74. Requiring Plaintiffs to constantly monitor all of the content on their sites and remove or segregate material that could be considered harmful to minors would impose a severe burden on Plaintiffs given the enormous quantity of speech on their sites and the fact that the content on the sites changes all the time, often every minute. Walsh Testimony, Oct. 23 Transcript, at 133:23-134:3.

3. Plaintiffs and Others Provide "Commercial" Web Pages.

75. Plaintiffs are commercial speakers on the Web. The speech on Plaintiffs' Web sites is designed to assist in making a profit. Although many of the Plaintiffs believe that much of the information available on their Web sites has non-commercial value, all of the information meets the definition of "for commercial purposes" under the Act. Walsh Testimony, Oct. 23 Transcript, at 112:20-21; Tepper Testimony, Oct. 30 Transcript, at 176:11-13; Glickman Testimony, Oct. 30 Transcript, at 92:12-13;

Griscom Testimony, Oct. 23 Transcript, at 52:25-53:1; Peckham Testimony, Oct. 31 Transcript, at 21:6-10; Corinna Testimony, Nov. 2 Transcript, at 100:1-5.

76. The Sexual Health Network is a for-profit corporation incorporated in the State of Connecticut. The headquarters of the corporation are located in Dr. Tepper's home in Connecticut. Tepper Testimony, Oct. 30 Transcript, at 176:5-13.

77. The Sexual Health Network primarily makes money through advertising on its Web site. The Sexual Health Network does not directly sell anything (other than advertising) on its site. Tepper Testimony, Oct. 30 Transcript, at 232:14-234:2, 235:17-19.

78. Urbandictionary.com is a commercial website, incorporated as a sole proprietorship by its founder, Aaron Peckham. Peckham Testimony, Oct. 31 Transcript, 23:6-10. It derives its income from advertising revenues, which are tied to the amount of traffic to its site. *Id.* at 45:11 to 46:5.

79. Scarleteen.com, scarletletters.com, and femmerotic.com are operated to make a profit. Corinna Testimony, Nov. 2 Transcript, at 100:2-5.

80. Art by various lesbian and gay artists, including Mr. Snellen's own works, are available for sale through the Leslie/Lohman Web site. Snellen Testimony, Nov. 2 Transcript, at 134:12-18, 143:24-144:25; P. Exh. 49.

81. Mr. Snellen and other artists have profited from selling art through the Leslie/Lohman Web site. Snellen Testimony, Nov. 2 Transcript, at 150:21-25.

82. The EAA operates a website, which it uses to promote and sell the works of its members. Lewis Testimony, Oct. 31 Transcript, at 90:25-91:22.

B. For Compelling Reasons, Plaintiffs and Other Web Speakers Do Not Restrict Access to Their Speech.

1. Access Restrictions Diminish Viewership.

83. Because the vast majority of content on the Web is available for free, most Web users will not provide payment cards or personal information simply to access a Web site. Walsh Testimony, Oct. 23 Transcript, at 161:25-162:11, 163:4-11, 170:7-11, 171:5-172:9, 173"10-20; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; A. Smith Testimony, Oct. 26 Transcript, at 188:24-189:10; Russo Testimony, Oct. 25 Transcript, at 146:14-148:16; Griscom Testimony, Oct. 23 Transcript, at 88:8-20; DeGenevieve Testimony, Nov. 1 Transcript, at 27:5-15; Snellen Testimony, Nov. 2 Transcript, at 135:25-140:4, 142:22-24, 143:15-23; S. Smith Testimony, Nov. 15 Transcript, at 189: 1-10. 217:1-218:14; P. Exh. 54, at 0373.

84. For additional facts on this subject, see *infra*, section on affirmative defenses, at II. B.

2. Providing Free, Unrestricted Access to Their Speech is Part of the Mission of Many Web Speakers.

85. Many of the Plaintiffs are committed to providing uncensored Web sites. Walsh Testimony, Oct. 23 Transcript, at 155:4-12 (Salon has not considered "toning down" the sexually explicit content of some of its material because "we really think the mix of topics that we present is what makes us Salon"); Glickman Testimony, Oct. 30 Transcript, at 133:15-134:2; Peckham Testimony, Oct. 31 Transcript, at 36:9-37:8.

86. The vast majority of information on Plaintiffs' Web sites, as on the Web in general, is provided to users for free. Walsh Testimony, Oct. 23 Transcript, at 161:4-6 (all of Salon's content is available today for free); Tepper Testimony, Oct. 30 Transcript,

at 194:13-15 (all of Sexual Health Network's content is available for free);Glickman Testimony, Oct. 30 Transcript, at 108:11-20; Griscom Testimony, Oct. 23 Transcript, at 64:5-9 (most of Nerve's content available for free); Peckham Testimony, Oct. 31 Transcript, at 55:22-56:6; Corinna Testimony, Nov. 2 Transcript, at 102:1-24.

87. The vast majority of information on Plaintiffs' Web sites, as on the Web in general, can be accessed without requiring users to register, provide a password or log-in, or otherwise provide any personal, identifying information in order to access the material. Walsh Testimony, Oct. 23 Transcript, at 138:16-22; Tepper Testimony, Oct. 30 Transcript, at 190:11-18; Peckham Testimony, Oct. 31 Transcript, at 30:12-18, 42:19-23.

88. Being able to communicate on the Web is critical to Plaintiffs and to the many other speakers who depend on the Web to express themselves as they see fit and to reach as large an audience as possible. Walsh Testimony, Oct. 23 Transcript, at 110:24-111:14; Tepper Testimony, Oct. 30 Transcript, at 177:6-19; A. Smith Testimony, Oct. 26 Transcript, at 194:18-195:21; Griscom Testimony, Oct. 23 Transcript, at 53:21-54:10; Peckham Testimony, Oct. 31 Transcript, at 23:18-25; Corinna Testimony, Nov. 2 Transcript, at 73:12-21, 74:16-22.

89. The Web is a unique forum and medium of communication because of its low barriers to entry and the fact that it enables heretofore unknown and un-established individuals to communicate with a vast worldwide audience. Walsh Testimony, Oct. 23 Transcript, at 110:24-111:5; Tepper Testimony, Oct. 30 Transcript, at 177:6-19; A. Smith Testimony, Oct. 26 Transcript, at 195:8-15; Griscom Testimony, Oct. 23

Transcript, at 53:21-54:10; Peckham Testimony, Oct. 31 Transcript, at 23:18-25; Corinna Testimony, Nov. 2 Transcript, at 73:12-21, 74:16-22.

90. The Web is also unique because it permits speakers to communicate on an unlimited variety of subjects and topics, many of which are far outside of the mainstream, and which would be very difficult to discuss in more traditional mediums of communication. Walsh Testimony, Oct. 23 Transcript, at 110:12-111:14; Corinna Testimony, Nov. 2 Transcript, at 73:12-21, 74:16-22.

91. Plaintiffs and many of the other speakers on the Web who will be affected by COPA seek to have older minors access their speech, and older minors currently access and contribute to the material on these Web sites. Walsh Testimony, Oct. 23 Transcript, at 113:3-19; Tepper Testimony, Oct. 30 Transcript, at 180:17-181:7; Corinna Testimony, Nov. 2 Transcript, at 74:5-9.

92. It is very important to many of the Plaintiffs and other speakers on the Web that their content be accessible to older minors, in part because older minors often do not have any other means of acquiring the information that Plaintiffs and these other speakers provide. Tepper Testimony, Oct. 30 Transcript, at 180:24-181:7; A. Smith Testimony, 217: 7-13; Corinna Testimony, Nov. 2 Transcript, at 74:16-24; Peckham Testimony, Oct. 31 Transcript, at 28:17-23.

93. The content on Plaintiffs' Web sites can be accessed by anyone with an Internet connection. Plaintiffs do not restrict the content on their Web sites to individuals over a certain age or to individuals in certain geographic locations. Walsh Testimony, Oct. 23 Transcript, at 113:20-24; Tepper Testimony, Oct. 30 Transcript, at 181:8-9, 194:16-17.

94. A significant number of the Internet users who access the material on Plaintiffs' Web sites are individuals who do not live in the United States. Walsh Testimony, Oct. 23 Transcript, at 113:23-114:19 ("we get roughly 20 percent of our traffic now from international readers"); Tepper Testimony, Oct. 30 Transcript, at 181:10-18 ("approximately 15 percent" of users come from overseas); Griscom Testimony, Oct. 23 Transcript, at 56:14-17 (15 percent of Nerve's visitors are from overseas); Peckham Testimony, Oct. 31 Transcript, at 25:14-17 (37 percent of Urban Dictionary's users are from overseas); Glickman Testimony, Oct. 30 Transcript, at 99:16-22.

95. It is extremely important to Plaintiffs to have the content on their sites available to Internet users who live outside the United States. Among other reasons, Plaintiffs want as many people as possible to access and discuss their speech, people who live overseas need this information just like people within the United States, and Plaintiffs desire to be part of the global conversation about the myriad of important issues affecting not just people in this country, but people from all over the world. Walsh Testimony, Oct. 23 Transcript, at 115:15-25; Tepper Testimony, Oct. 30 Transcript, at 181:19-23; Peckham Testimony, Oct. 31 Transcript, at 25:18-25.

96. Because they believe that their speech is valuable and necessary and that it provides people with free information and resources that are not available from other sources, it is critical to Plaintiffs that their speech be accessible by as many people as possible. Walsh Testimony, Oct. 23 Transcript, at 163:10-164:2; Tepper Testimony, Oct. 30 Transcript, at 180:24-181:7, 181:19-23; Griscom Testimony, Oct. 23 Transcript, at 84:24-85:13; Peckham Testimony, Oct. 31 Transcript, 55:17 to 56:6.

97. In addition to selling products for profit, Condomania aims to educate consumers about issues relating to safer sex and to provide a safe and private environment for its customers to learn about and purchase safer sex and romance products. Glickman Testimony, Oct. 30 Transcript, at 94:18-95:10.

98. Dr. Tepper founded the Sexual Health Network in 1996. The Sexual Health Network was founded to fulfill the mission of providing easily accessible sexual health information to people with disabilities and chronic conditions, and to end the silence around issues of sexual health as they interact with people's medical conditions. Tepper Testimony, Oct. 30 Transcript, at 176:18-177:5; Defendant's Exhibit ("D. Exh.") 111.

99. Dr. Tepper decided to publish his information on the Web in order to make information that was previously hard to find easily accessible to the people who needed that information. Communicating on the Web is especially critical for the Sexual Health Network because the Web gives people with disabilities unparalleled access to the same information as people without disabilities, and eliminates the everyday physical accessibility issues that people with disabilities otherwise have to face. It also enables individuals to obtain this sensitive and, for some, embarrassing information anonymously. Tepper Testimony, Oct. 30 Transcript, at 177:6-178:23.

100. Appropriateness for minors is not a consideration for the Sexual Health Network in determining what material to make accessible on its Web site. Tepper Testimony, Oct. 30 Transcript, at 183:23-25.

101. The Sexual Health Network does not restrict access to the content on its Web site to anyone, because the content is there for anyone who has an interest or a need for the content, and because the Sexual Health Network does not want to restrict access

to information that is potentially life enhancing or life-saving. Tepper Testimony, Oct. 30 Transcript, at 194:16-22.

102. Public health educators know that the majority of minors have engaged in sexual behaviors that put them at some sort of health risk by the time they are 17 years old. It is very important for older minors, and for some younger minors, to be able to access the Sexual Health Network's speech, because the information provided is about important health issues facing many older minors, and because older minors often do not have many other venues to access this information about which they are curious or concerned. Tepper Testimony, Oct. 30 Transcript, at 180:24-181:7, 198:23-199:10; P. Exh. 37, at 89 (question from 11 year-old).

103. Urbandictionary.com is committed to providing its content to users for free, and charging money for access to its content would be inconsistent with its mission of documenting the world's English and making it as accessible as possible to all people. Peckham Testimony, Oct. 31 Transcript, 55:17 to 56:6.

104. Urbandictionary.com does not require its users to supply personal information in order to contribute to the site. To post a word or definition, a user must provide only a working email address. Peckham Testimony, Oct. 31 Transcript, 30:12-18. To view the site or to vote on a definition, a user need not supply any information at all. *Id.* at 42:19-23.

105. Scarletletters.com is published online, in part, in order to reach the widest possible audience. Corinna Testimony, Nov. 2 Transcript, at 73:12-19.

106. Scarleteen.com's content is available for free. Corinna Testimony, Nov. 2 Transcript, at 74:10-11.

107. All of the content on scarletletters.com that has been placed on the site in the last two years is available to anyone for free. Corinna Testimony, Nov. 2 Transcript, at 126:2-127:9.

108. Much of the content on femmerotic.com is available for free. Corinna Testimony, Nov. 2 Transcript, at 95:25-96:1.

109. It is important to the mission of both scarleteen.com and scarletletters.com that their content be provided for free so as to reach a large number of people. Corinna Testimony, Nov. 2 Transcript, at 102:3-24.

110. The Leslie/Lohman Foundation's mission is to show and exhibit work by gay and lesbian artists, in the Gallery and online through the Foundation's Web site (www.Leslie.Lohman.org), that is generally not shown in galleries or otherwise available to the general public due to the sexual content or the sexual orientation of the artist. Snellen Testimony, Nov. 2 Transcript, at 130:4-131:3, 131:19-132:13, 133:16-20.

111. Free, unrestricted access to the Leslie/Lohman Web site is essential to the Foundation's mission, as anonymity is important to the Web sites' visitors, and requiring any kind of personal information before accessing the content would deter more people than it would attract. Snellen testimony, Nov. 2 Transcript, at 139:18-140:20, 142:22-143:23.

112. Ms. Smith has her own Web site, god-des.com. Users can listen to her songs, watch videos of her performing, and purchase her albums on her site and on other sites on the Web, including her myspace.com Web page. Written lyrics to her songs are available on the Web as well. A. Smith Testimony, Oct. 26 Transcript, at 195:22-197:4, 198:15-20, 206:8-16.

113. Ms. Smith's Web site can be accessed by anyone worldwide who has an Internet connection. She does not charge a fee to visitors, or require any personal information before a user can enter the Web site, and has no desire to do so because she wants as many people as possible to find out about her and hear her songs. A. Smith Testimony, Oct. 26 Transcript, at 196:6-197:14.

114. It is important for Ms. Smith's lyrics to be as sexually explicit as they are in order for her to convey her artistic message. Much of hip-hop and rap is focused on sex, from the male perspective. Ms. Smith uses sexually explicit language and lyrics in order to provide a counter to those messages, and to sing about female pleasure. A. Smith Testimony, Oct. 26 Transcript, at 183:13-24, 207:15:208:8, 208:20-209:14.

115. Many of Ms. Smith's fans are minors. A. Smith Testimony, Oct. 26 Transcript, at 184:17-24.

116. The fact that Ms. Smith's fans cannot buy her music in stores has caused problems for many of her fans. Many of her fans have contacted her in an attempt to find out if they can buy her albums in stored instead of on the Web because they either do not want to give out their credit card information online or they do not have a credit card. A. Smith Testimony, Oct. 26 Transcript, at 188:24-189:10.

3. Providing Free, Unrestricted Access is Essential to the Commercial Success of Many Web Speakers.

117. Plaintiffs, like the universe of commercial speakers on the Web, have a variety of business models. Some of the Plaintiffs receive income by selling advertising on their Web sites. Some of the Plaintiffs sell goods over their Web sites, ranging from millions of books, to condoms and other sexual health devices, to books that they authored themselves. Some of the Plaintiffs use the Web simply as an advertising and

marketing tool -- a means of promoting their commercial activities. Some of the Plaintiffs generate revenue by combining these or utilizing other business models. Walsh Testimony, Oct. 23 Transcript, at 157:16-158:4 ("Primarily, we make money now with online advertising," and discussing other revenue streams), 159:3-5 (advertising revenues are "crucial" to Salon); Tepper Testimony, Oct. 30 Transcript, at 232:14-233:2; Glickman Testimony, Oct. 30 Transcript, at 92:8-23, 94:12-95:1, 98:8-11; Griscom Testimony, Oct. 23 Transcript, at 81:17-82:11; Peckham Testimony, Oct. 31 Transcript, at 45:11-46:5; Corinna Testimony, Nov. 2 Transcript, at 100:6-101:3.

118. Web sites, including Plaintiffs' Web sites, depend on attracting a high level of traffic to their sites to attract and retain advertisers and investors. Walsh Testimony, Oct. 23 Transcript, at 158:10-24 (traffic is "very important" to Salon's advertising revenues); Tepper Testimony, Oct. 30 Transcript, at 233:3-23 (traffic is "critical" to advertising revenues); Griscom Testimony, Oct. 23 Transcript, at 82:12-83:14; Peckham Testimony, Oct. 31 Transcript, at 45:11-46:5.

119. The best way to stimulate user traffic on a Web site is to offer some content for free to users. Walsh Testimony, Oct. 23 Transcript, at 171:5-8 ("The vast majority" of Internet users are not willing to pay to access Salon's content); Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; Griscom Testimony, Oct. 23 Transcript, at 84:9-24 (Nerve's premium subscribers are attracted to the site by free content); Snellen Testimony, Nov. 2 Transcript, at 136:2-18; S. Smith Testimony, Nov. 15 Transcript, at 179:15-180:6.

120. The vast majority of the people who visit Plaintiffs' Web sites will not pay simply to access the content on the Web sites. Walsh Testimony, Oct. 23 Transcript, at

168:11-14 (roughly two percent of users pay to become premium members), at 171:5-8 ("A small minority of Salon readers are willing to pay. The vast majority are not willing to pay."); Griscom Testimony, Oct. 23 Transcript, at 66:1-17 (fewer than one percent of Nerve's readers are paid subscribers).

121. The number of Internet users who visit Plaintiffs' and other speakers' Web sites is also critical to their ability to make money, because, among other things, the more traffic a site has, the higher its advertising rates can be and the higher its advertising revenues will be. Walsh Testimony, Oct. 23 Transcript, at 117:2-9; Griscom Testimony, Oct. 23 Transcript, at 82:12-83:14; Peckham Testimony, Oct. 31 Transcript, at 46:1-5.

122. Eliminating the sexually explicit content on Plaintiffs' Web pages will significantly reduce the traffic to their sites given the popularity of that content. Walsh Testimony, Oct. 23 Transcript, at 143:8-16; A. Smith Testimony, Oct. 26 Transcript, at 217:1-13.

123. Because the Web is still a relatively new medium of communication, Plaintiffs, like other entities using the Web for commercial purposes, need to be able to adapt and modify their business plans and business models quickly and often, depending on trends in the industry and unexpected changes. Walsh Testimony, Oct. 23 Transcript, at 1134:21-135:14.

124. With respect to those Plaintiffs and others who sell goods on their Web sites, only a small percentage of Internet users who visit those Plaintiffs' sites for information actually make a purchase. Glickman Testimony, Oct. 30 Transcript, at 97:14-99:9.

125. For example, of the approximately 4000 unique visitors to www.condomania.com each day, only approximately 2.5 percent make a purchase. Maintaining and growing the number of visitors to www.condomania.com is crucial to the success of Condomania's business. Glickman Testimony, Oct. 30 Transcript, at 97:14-99:9.

126. It is crucial to both Condomania's business and educational missions that all of the Web pages on www.condomania.com are available for visitors to view for free. This allows Condomania to provide information to its visitors and attract new customers. Glickman Testimony, Oct. 30 Transcript, at 108:11-20.

127. It is not feasible for Condomania to determine which material on its Web pages is more likely to be considered "harmful to minors" and then segregate that content behind an age verification screen because the material Condomania believes most likely to be covered by Section 231(e)(6)(B) of the Act is inextricably interwoven with content it believes to be less likely to be covered by the Act. It would be counter to Condomania's business and educational missions, which attempt to situate safer sex and romance related products alongside frank discussions regarding their use, to remove or segregate the frank and explicit discussions of sexual topics from its Web pages. Glickman Testimony, Oct. 30 Transcript, at 133:15-134:2.

C. Plaintiffs and Other Web Speakers Are Reasonably Chilled by COPA.

128. Plaintiffs believe that all of their speech has value, especially for adults and older minors. Walsh Testimony, Oct. 23 Transcript, at 138:11-16; Tepper Testimony, Oct. 30 Transcript, at 203:1-6; Glickman Testimony, Oct. 30 Transcript, at 131:18-23, 132:13-133:10; Griscom Testimony, Oct. 23 Transcript, at 58:14-59:4;

Peckham Testimony, Oct. 31 Transcript, at 28:10-23, 36:21-37:8; Corinna Testimony, Nov. 2 Transcript, at 88:19-21, 90:1-2, 97:10-12.

129. Plaintiffs all fear prosecution under COPA for the content on their Web sites. J. Exh. 1, ¶30, 32.

130. Although Salon believes its speech has value, even for older minors, Salon reasonably believes that many others do not share that view. Walsh Testimony, Oct. 23 Transcript, at 137:15-138:2 (discussing why Salon's content might be considered by some to be harmful to minors), 153:25-154:4 (COPA uses a "very subjective standard" so "I'm sure other parents would not be" fine to have their children view Salon's content). Indeed, Salon has received complaints because of the sexually explicit nature of the content on its Web site. Walsh Testimony, Oct. 23 Transcript, at 154:19-22. Salon has also suffered financial consequences, including lost advertising, because of the sexually explicit nature of its content. Walsh Testimony, Oct. 23 Transcript, at 155:13-156:4.

131. Because Salon publishes sexually explicit articles and images, Salon reasonably fears that its speech might be considered harmful to minors, and that it might be prosecuted under COPA for making that content available on its Web site. Walsh Testimony, Oct. 23 Transcript, at 137:15-138:2, 153:18-24, 157:4-15; P. Exh. 39, at 1-5, 61-63, 75-78, 64-74, 94-100, 101-111, 119-135.

132. Although Salon does not publish its sexually explicit speech with the goal of being "patently offensive" or pandering to the prurient interest of adults or minors, Salon understands and knows that its content will be considered by many people to be offensive. Walsh Testimony, Oct. 23 Transcript, at 183:17-20.

133. Although Condomania believes its speech on www.condomania.com has value, even for older minors, Condomania reasonably believes that many others do not share that view and may consider its speech to be "harmful to minors". Glickman Testimony, Oct. 30 Transcript, at 131:18-23, 132:13-133:10.

134. Although Nerve believes its speech has value, even for older minors, Nerve reasonably believes that many others do not share that view. Griscom Testimony, Oct. 23 Transcript, at 80:7-17.

135. Although Urban Dictionary believes its speech has value, even for older minors, Urban Dictionary reasonably believes that many others do not share that view. Peckham Testimony, Oct. 31 Transcript, at 44:25-45:7.

136. Urban Dictionary's book publisher would not allow him to include words about sex in his book. Peckham Testimony, Oct. 31 Transcript, at 78:6-79:9.

137. Although the Sexual Health Network believes its speech has value, even for older minors, the Sexual Health Network reasonably believes that many others do not share that view. The Sexual Health Network believes that many others will not share its views given, among other reasons: the past governmental enforcement of certain obscenity laws, such as the Comstock laws, against non-obscene, but sexually focused, material such as contraception and abortion information; the U.S. government's abstinence-only-until marriage sexual education policy, under which educators and schools receiving federal funding are prohibited from discussing many topics related to sexuality, such as how to use condoms or to engage in safe sex; the controversy and sudden departure from government of former Surgeon General Jocelyn Elders after she publicly discussed the concept of discussing masturbation in schools; the trouble,

controversy and threats that college and high school professors and teachers of sexual education have encountered over the years due to the sexually explicit and controversial, allegedly inappropriate, nature of the topics that are discussed in their classes; and the personal resistance that Dr. Tepper has encountered from the school of his own child and from the parents of his son's friends and classmates, who are concerned about what Dr. Tepper does for a living and do not want him to speak to the children about his work. Tepper Testimony, Oct. 30 Transcript, at 197:3-203:13.

138. Because the Sexual Health Network makes sexually explicit information available on its Web site, the Sexual Health Network reasonably fears that its speech might be considered harmful to minors, and that it might be prosecuted under COPA for making that content available on its Web site. Tepper Testimony, Oct. 30 Transcript, at 197:3-203:13, 230:12-231:13.

139. The Sexual Health Network's fear of prosecution is accentuated by the fact that "educational value" is not included in the third prong of COPA's definition of "harmful to minors," such that even if its speech is deemed to have educational value for minors, the Sexual Health Network would still be subject to prosecution under COPA. Tepper Testimony, Oct. 30 Transcript, at 230:12-231:13.

140. The operator of scarletletters.com believes the content is not appropriate for minors and has included a "splash page" to warn visitors of the content. Corinna Testimony, Nov. 2 Transcript, at 86:20-87:24.

141. The operator of scarleteen.com believes she is at risk in part because the government "has made clear that the sex information I give to teenagers isn't what they want in schools . . .." Corinna Testimony, Nov. 2 Transcript, at 76:7-17.

142. Although Mr. Snellen believes the speech on Leslie/Lohman Web site has value for older minors, he reasonably believes that many others do not share that view, as community standards for what is appropriate for young people to view differs in places like New York and Missouri. The art on the Leslie/Lohman Web site depicts sexual acts that many people might consider pornographic. Snellen Testimony, Nov. 2 Transcript, at 151:4-152:2, 158:17-159:11.

143. Mr. Snellen's experience with artists who have had their art removed from the Internet by an Internet Service Provider without warning, the Foundation's receipt of letters indicating God would not approve of the art work displayed and would consider it pornographic, as well as the forced closure of a Robert Mapplethorpe exhibit in Cincinnati and the subsequent prosecution of the curator because of the sexual content of the exhibit, inform Mr. Snellen's fear of prosecution for the art on the Leslie/Lohman Web site if COPA were to take effect. Snellen Testimony, Nov. 2 Transcript, at 151:4-154:21.

144. Although Ms. Smith believes her speech has value, especially for older minors, she reasonably believes that many others in this country do not share that view. Ms. Smith's fear of prosecution for the songs she makes available on the Web stems from her experiences in which she has been prohibited from performing certain songs in public places where families and kids are present, even in places like New York City, from the comments and complaints she has received due to the sexually explicit nature of her songs, and from the fact that her sexually explicit songs, like Lick-It, cannot get played on the radio. A. Smith Testimony, Oct. 26 Transcript, at 190:2-19, 200:25-202:16.

145. Although Ms. Lewis believes the speech on the EAA website has value for adults, she reasonably believes that many others do not share that view. Lewis Testimony, Oct. 31 Transcript, at 96:04-108:25.

146. Although Professor DeGenevieve believes her speech has value, even for older minors, she reasonably believes that many others do not share that view. DeGenevieve Testimony, Nov. 1 Transcript, at 56:19-57:5, 58:17-59:5; P. Exh. 53.

147. Professor DeGenevieve lost an NEA grant due to the sexually explicit nature of her speech. Based on this experience, Professor DeGenevieve reasonably fears that some communities and even the Federal government may find her work to be "harmful to minors." DeGenevieve Testimony, Nov. 1 Transcript, at 18:4-22:15.

148. Professor DeGenevieve reasonably believes that her artwork is covered by Section 231 (e)(6)(B) of the Act's definition of "material that is harmful to minors" and if the Act were to take effect, her fear of prosecution is reasonable based on the content of the Web pages on www.degenevieve.com. DeGenevieve Testimony, Nov. 1 Transcript, at 58:7-59:15.

149. The chill felt by Plaintiffs and the other Web speakers is all the more reasonable in view of the fact that speech similar to that of Plaintiffs and the other Web speakers has been the subject of extensive efforts at censorship and prosecution across the country historically and, more particularly, in recent years. Reichman Testimony Oct. 30 at 22:2-6; P. Exh. 22; DeGenevieve Testimony, Nov. 1 Transcript, at 18:4-22:15; Snellen Testimony, Nov. 2 Transcript, at 151:4-154:21.

150. The chill felt by Plaintiffs and the other Web speakers is reasonable in view of the fact that many of them have personally received complaints about the sexual

nature of their speech. Walsh Testimony, Oct. 23 Transcript, at 156:19-157:15; Glickman Testimony, Oct. 30 Transcript, at 132:24-133:10; DeGenevieve Testimony, Nov. 1 Transcript, at 22:13-15; Snellen Testimony, Nov. 2 Transcript, at 153:3-17.

151. That the statute is overbroad and the chill felt by Plaintiffs and the other Web speakers is reasonable is also demonstrated by the fact that at least one Web page from each of the Plaintiffs' Web sites is blocked by at least two of the major filtering products, reflecting a consensus view that these speakers engage in at least some speech that is inappropriate for minors. D. Exh. 85; Mewett Testimony, Nov. 7 Transcript, at 131:23-133:19; J. Exh. 1, ¶32, 85.

152. That the statute is overbroad and the chill felt by Plaintiffs and the other Web speakers is reasonable is also demonstrated by the fact that some of the major filtering products "attempt to block terms like gay and lesbian," reflecting a consensus view that these words and ideas are inappropriate for minors. Mewett Testimony, Nov. 8 Transcript, at 58:26-59-1.

153. That the statute is overbroad and the chill felt by Plaintiffs and the other Web speakers is reasonable is also demonstrated by the fact that in conducting their filtering study, Defendant's experts found a substantial number of Web pages whose categorization "most definitely" required judgment, which were categorized differently by different human reviewers, and whose categories were subsequently changed after further review by another reviewer. Mewett Testimony, Nov. 7 Transcript, at 118:14-16, 233:16-235:3; P. Exh. 178.

154. That the statute is overbroad and the chill felt by Plaintiffs and the other Web speakers is reasonable is also demonstrated by the fact that even though

Defendant's experts created their own definitions of sexually inappropriate content and did not rely on the vague statutory language, Defendant's experts found it necessary to create a category of "other" for Web pages that could not be placed into any specific category. Mr. Mewett variously described these pages as "grey areas" or "really close" or "darker rather than lighter" or Web pages that "some people would probably characterize as adult entertainment" or about which "reasonable people could disagree." Mewett Testimony, Nov. 7 Transcript, at 219:14-220:21; P. Exh. 176.

155. Some of the Plaintiffs' Web pages were categorized by Mr. Mewett as "other." The "other" category created by Defendant's Mewett/Stark study contained 600-700 Web pages. Mewett Testimony, Nov. 7 Transcript, at 221:6-7, 220:8-11; P. Exh. 168-170.[1]

156. The Web pages categorized by Defendant's Mewett/Stark study as "other" are examples of Web pages that would reasonably be chilled. The "other" category provides rough evidence that, even with criteria defined and applied by one person, for all of those sites that are accurately categorized as sexually explicit, an additional 50% would be reasonably chilled. Mewett Testimony, Nov. 7 Transcript, at 220:8-11; P. Exh. 168-170.

157. That the statute is overbroad and the chill felt by Plaintiffs and the other Web speakers is reasonable is also demonstrated by the fact that even though Defendant's experts created their own definitions of sexually inappropriate, their application of those definitions in their categorizations were inconsistent. For example,

[1] This fact can be seen in any of the Master Databases in Exhibits 168-170. For example, in the "Supplemental Revised Master Database" on the CD containing Plaintiffs' Exhibit 170, each table contains a column marked "5G" or Mewett's "other" category. Each time Mewett marked a URL "other" it was noted in this column.

Mr. Mewett testified that a Web page showing an oil painting of bestiality could never be "sexually explicit" because it was artistic (a category he created to exempt otherwise sexually explicit Web pages, analogous to 47 USC 231(e)(6)(C)), but that an art work by Michelangelo would not be artistic. Mewett Testimony, Nov. 7 Transcript, at 235:21-236:12, Nov. 8 Transcript, at 22:15-24:4. As another example, Mr. Mewett did not categorize the National Center for Lesbian Rights as political (a category he created to exempt otherwise sexually explicit Web pages, analogous to 47 USC 231(e)(6)(C)). Mewett Testimony, Nov. 7 Transcript, at 229:1-23; P. Exh. 177, p. 8. Mr. Mewett further testified that he properly categorized the Gay and Lesbian Medical Association (or even the Heterosexual Medical Association) as Web pages containing sexual content or nudity. Mewett Testimony, Nov. 7 Transcript, at 230:25-232:6; P. Exh. 178, p. 10.

158. The reasonableness of the chill felt by Plaintiffs and the other Web speakers was confirmed by Professor Reichman. Reichman Testimony Oct. 30 Transcript, at 46:24-47:14; P. Exh. 22, 23.

159. Professor Reichman is an expert in censorship and the suppression of speech. Reichman Testimony, Oct. 30 Transcript, at 18:2-20.

160. Professor Reichman publishes a newsletter for the American Library Association that details instances of challenges to intellectual freedom. Reichman Testimony, Oct. 30 Transcript, at 8:1-19; P. Exh. 23.

161. The categories of speech most often targeted for censorship are those about sex. Reichman Testimony, Oct. 30 Transcript, at 14:15-19.

162. Professor Reichman has documented approximately 1,500 instances of attempted censorship of speech about sex over the last 25 years. Reichman Testimony, Oct. 30 Transcript, at 11:9-10, 15:1-8; P. Exh. 23.

163. ALA has documented approximately 5,718 challenges to materials in schools and libraries during the 1990's. Of those, 1,446 were to materials deemed sexually explicit, 1,262 contained language deemed offensive, and 1,167 were "unsuited to age group." Reichman Testimony, Oct. 30 Transcript, at 21:3-23.

164. Challenges to speech that are initiated by private citizens are relevant to COPA because they create a chill among speakers, because they may put pressure on government to act either as a result of the pressure or to avoid a costly battle, and because COPA contains a civil cause of action. Reichman Testimony, Oct. 30 Transcript, at 19:18-20:22.

165. Categories of speech about sex that are routinely challenged in schools and libraries include sex education, sexually oriented fiction, and gay and lesbian materials. Reichman Testimony, Oct. 30 Transcript, at 22:2-6; P. Exh. 22.

166. There are many examples of speech that was challenged in schools and libraries that involved sex education. Among those examples are one in 2004 in South Dakota when the Governor ordered the removal of links to sex education sites from the state library website, a 2002 decision by a library board in Iowa to ban a sex education book, and a 2001 decision by a school board in Alaska to restrict access to a sex education book. Many other such examples are listed in Professor Reichman's expert report. Reichman Testimony, Oct. 30 Transcript, at 22:7-25:12; P. Exh. 22 at 15-18; P. Exh. 23.

167. Plaintiffs' Web sites, including Sexual Health Network, Scarleteen.com, and Condomania, contain speech similar to that and even "more sexually explicit" than materials that have been challenged in schools and libraries. Reichman Testimony, Oct. 30 Transcript, at 25:13-23; P. Exh. 22 at 15-18; P. Exh. 23.

168. There are many examples of speech that was challenged in schools and libraries that involved sexually oriented fiction, including very highly regarded fiction. Among those examples are a school district in California that removed a book discussing a first sexual experience, a school board in Pennsylvania that removed a book discussing gay male arousal, a school district in Oklahoma that restricted certain novels, and a school district in California that removed a book describing a teenage girl's "description of how her breasts react to the cold." Reichman Testimony, Oct. 30 Transcript, at 25:24-30:6; P. Exh. 22 at 18-24; P. Exh. 23.

169. Plaintiffs' Web sites, including scarletletters.com and Nerve, contain speech similar to and even "more explicit" than materials that have been challenged in schools and libraries. Reichman Testimony, Oct.30 Transcript, at 30:7-19.

170. There are many examples of speech that was challenged in schools and libraries that involved gay or lesbian people. Among those examples are a resolution by the Oklahoma House of Representatives urging the banning of a fairy tale book about gay marriage, a Hawaii school board that restricted a video about discrimination against gay and lesbian people, a high school editor in California removed from his post for publishing an article about gay students, and an Oklahoma resolution of the House of Representatives urging libraries to confine "homosexually-themed books" to areas for

adult access only. Reichman Testimony, Oct. 30 Transcript, at 30:20-32:6; 32:13-33:22, 34:6-35:23; P. Exh. 22 at 24-28; P. Exh. 23.

171. Plaintiffs' Web sites, including scarletletters.com, nerve.com, Philadelphia Gay News, and scarleteen.com contain speech similar to and even "more explicit" than materials that have been challenged in schools and libraries. Reichman Testimony, Oct. 30 Transcript, at 38:10-19.

172. It is useful in determining the propensity of people to censor materials for minors to look at attempts to censor material in schools. Reichman Testimony, Oct. 30 Transcript, at 52:9-20.

173. The motion picture rating system represents a consensus of what many people believe is appropriate for minors to view, and it makes a distinction between older and younger minors. Reichman Testimony, Oct. 30 Transcript, at 38:20-41:1; P. Exh. 22 at 10-13.

174. The television indecency enforcement by the FCC is relevant in showing what material the federal government believes is inappropriate for minors. Reichman Testimony, Oct. 30 Transcript, at 41:2-21; P. Exh. 22 at 13-14.

175. Based on the history of censorship in this country, including the numerous examples documented in Professor Reichman's testimony and in his expert report, Plaintiffs have a reasonable fear that their expression would be chilled if COPA were applied to them. Reichman Testimony, Oct. 30 Transcript, at 46:24-47:14; P. Exh. 22, 23.

D. COPA is Impermissibly Vague.

1. Plaintiffs Cannot Determine What Speech is Covered by COPA.

176. Plaintiffs and other Web speakers cannot determine what speech is and is not covered by the statute. Griscom Testimony, Oct. 23 Transcript, at 56:23-58:2; Walsh Testimony, Oct. 23 Transcript, at 135:22-137:5; Glickman Testimony, Oct. 30 Transcript, at 130:3-22; Tepper Testimony, Oct. 30 Transcript, at 195:14-197:2; Peckham Testimony, Oct. 31 Transcript, at 27:12-23; Lewis Testimony, Oct. 31 Transcript, at 95:2-96:3; Corinna Testimony, Nov. 2 Transcript, at 75:20-76:6.

177. If COPA is not permanently enjoined, some of the Plaintiffs intend to self-censor; others intend to risk liability and prosecution under the Act; and others have not yet decided what they will do. Walsh Testimony, Oct. 23 Transcript, at 173:21-24 ("I honestly don't know. I really don't know what we would do."); Tepper Testimony, Oct. 30 Transcript, at 243:7-17; Glickman Testimony, Oct. 30 Transcript, at 136:13-18; Griscom Testimony, Oct. 23 Transcript, 55:17 to 56:6, at 91:9-17; Corinna Testimony, Nov. 2 Transcript, at 104:17-24 (Heather Corinna would risk prosecution to continue publishing scarleteen.com); Peckham Testimony, Oct. 31 Transcript, at 56:17-24 ("I'm not sure what I would do.").

178. Plaintiffs' inability to understand what speech is covered by the statute stems, in great part, from the fact that the statute relies on terms that are subjective in nature, and because many people in this country disagree about what is appropriate and not appropriate for minors to view when it comes to speech that is sexually explicit in nature. Walsh Testimony, Oct. 23 Transcript, at 135:22-136:2; Tepper Testimony, Oct. 30 Transcript, at 195:14-22.

179. The Sexual Health Network does not know exactly what speech is harmful to minors under COPA, in great part because there is much disagreement in the country, even within professional educators and academics in the sexual health and sexual education fields, as to what is appropriate or not appropriate for minors when it comes to sexually explicit speech and sexual education. Tepper Testimony, Oct. 30 Transcript, at 195:14-22, 230:12-231:13.

180. Understanding what it means for speech to be "prurient with respect to minors" is especially confusing and difficult for the Sexual Health Network, because even professionals in the sexual health and education field disagree about how to determine whether something is "prurient" for adults, let alone for minors. Tepper Testimony, Oct. 30 Transcript, at 196:7-17.

181. Plaintiffs do not know which community's standards will determine whether its speech is harmful to minors. Walsh Testimony, Oct. 23 Transcript, at 138:3-10.

182. Community standards differ within regions of the United States and other countries. Alexander Testimony, Nov. 13 Transcript, at passim; Mewett Testimony, Nov. 7 Transcript, at 201:9-12; Snellen Testimony, Nov. 2 Transcript, at 151:10-16.

183. To the extent Defendant proffered Quova as a solution to the vagueness and over breadth of the "community standards" section of COPA, it will not work. If Quova were used to block access to certain locations, it would require the speaker to block all persons in that location, including adults as well as minors. Alexander Testimony, Nov. 13 Transcript, at 34:14-23.

184. To the extent Defendant proffered Quova as a solution to the vagueness and over breadth of the "community standards" section of COPA, it will not work. The cost of Quova's product ranges from $6,000-$24,000 per year. Alexander Testimony, Nov. 13 Transcript, at 36:8-37:6.

185. To the extent Defendant proffered Quova as a solution to the vagueness and over breadth of the "community standards" section of COPA, it will not work. Quova cannot determine the location of a reader if that reader is accessing a Web page through AOL, a corporate proxy, a proxy server, mobile devices, or long distance dial-up. Therefore, in order to ensure that no reader from a particular locality accesses a Web page, Quova would have to block access to anyone using any of those means of access. Alexander Testimony, Nov. 13 Transcript, at 34:24-36:7; P. Exh. 54, at 93.

186. To the extent Defendant proffered Quova as a solution to the vagueness and over breadth of the "community standards" section of COPA, it will not work. Quova cannot reliably distinguish among readers by state if the readers are close to the state border. Alexander Testimony, Nov. 13 Transcript, at 28:8-16.

2. Defendant Cannot Describe What Speech is Covered by COPA.

187. Other than the express words of the statute, Defendant has no policies, guidelines, criteria, or rationales for interpreting what speech is harmful to minors, but not obscene. P. Exh. 166, 167; 165 Attachments A, B and CD-ROM.

188. Because Defendant has no policies, guidelines, criteria, or rationales for determining whether certain material is harmful to minors, a Web site operator has no means of determining whether its Web site is covered by COPA other than by looking at the express words of the statute. P. Exh. 166, 167; 165 Attachments A, B and CD-ROM.

189. Defendant is unable to define speech covered by COPA. His determination of when the depiction of a post-pubescent female breast on a Web page is sufficient to constitute a violation of COPA is so irrational as to constitute an admission that he cannot define COPA. According to Defendant, photographs of topless women exposing post-pubescent breasts can be harmful to minors in certain circumstances and not harmful to minors in other ill-defined contexts. According to Defendant, a photograph of topless women exposing post-pubescent breasts on Playboy.com's Web page is not harmful to minors. According to Defendant, a photograph of topless women exposing post-pubescent breasts on Penthouse.com's Web page is harmful to minors. According to Defendant, a photograph of a topless woman exposing post-pubescent breasts, where the nipples are covered by superimposed "stars," is harmful to minors. 47 USC 231(e)(6)(B); P. Exh. 166, 167 Interrogatory 15; P. Exh. 165 Attachments A, B and CD-ROM.

190. Defendant is unable to define speech covered by COPA. COPA defines a minor as someone under the age of 17, and thus implicitly defines an adult as someone 17 or above. The Defendant admits that there is no meaningful distinction between speech that is harmful to 16 year olds and speech that is obscene for 17 year olds. Speech covered by COPA is essentially speech that is obscene "for minors." Defendant admits that there is no speech that meets the definition of COPA (based on a 16 year old) that does not also meet the definition of obscenity (based on a 17 year old). P. Exh. 166, Interrogatories 7-9; P. Exh. 167, Interrogatories 7-9.

191. Defendant is unable to define speech covered by COPA. Defendant's assertion that none of the speech engaged in by the plaintiffs is "prurient" is so patently

false as to constitute an admission that he cannot define prurience under COPA. 47 USC 231(e)(6)(A); P. Exh. 166 and 167, Interrogatory 12; P. Exh. 165, Attachment A, pp. 0019-0107.

192. Defendant is unable to define speech covered by COPA. Defendant's assertion that none of the speech engaged in by the plaintiffs "depicts, describes, or represents an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the post-pubescent female breast" is so patently false as to constitute an admission that he cannot define this section of COPA. 47 USC 231(e)(6)(B); P. Exh. 166 and 167, Interrogatory 13; P. Exh. 165, Attachment A, pp. 0019-0107.

193. The Defendant is unable to define speech covered by COPA. In attempting to do so, he relies on a definition of "as a whole" (47 USC 231(a)(1) that is contradicted by the undisputed evidence, including evidence from his own witnesses. Without resort to his erroneous definition of "as a whole," Defendant's attempt to define the terms of the statute is irrational. For evidence that Web page, not Web site, is the proper definition of "as a whole," see J. Exh. 1 at ¶¶79-84; Felten Testimony, Oct. 25 Transcript, at 34:25-35:7; Stark Testimony, Nov. 8 Transcript, at 164:18-25; Mewett Testimony, Nov. 7 Transcript, at 206:12-207:18; Peckham Testimony, Oct. 31 Transcript, at 48:22-25, 51:3-6 (60 percent of visitors don't go through homepage and 50 percent visit only one page). For evidence that Defendant relies on a definition of "as a whole" to define the specific terms of COPA, see P. Exh.166 and 167, Interrogatories 11-15, 17-18.

194. Because of the increased use of search engines, whose purpose it is to accurately guide users to Web pages they wish to view, it is less likely than in 1998 that people will accidentally encounter pornography. Oct. 25 Transcript, at 32:1-20.

195. Defendant has previously admitted that COPA is vague, and argued against its enactment because of its vagueness. P. Exh. 55 at 000004-6.

II. COPA'S AFFIRMATIVE DEFENSES DO NOT CURE ITS DEFICIENCIES.

A. In General.

196. In the physical world, assessing the validity of an assertion about a person's age is relatively straightforward because of face-to-face interactions. Someone seeking to purchase harmful-to-minors material can be asked to show identification indicating the purchaser's age. The provider can compare this identification to the person presenting it. That level of assurance is not available in the absence of face-to-face interactions, such as when users access a Web page. P. Exh. 25, at 0030-0031; P. Exh. 54, at 0088, 0091-92.

197. There are no age verification services or products available to Web sites that actually verify the age of Internet users. There are no services or products that can effectively prevent access to Web pages by a minor. Russo Testimony, Oct. 25 Transcript, at 120:6-11, 124:1-6, 157:3-158:8, 164:15-165:7; 166:14-167:12; Tepper Testimony, Oct. 30 Transcript, at 234:13-15; Peckham Testimony, Oct. 31 Transcript, at 48:7-9; Cadwell Testimony, Oct. 31 Transcript, at 163:18-164:1, 174:17-175:16; Meiser Testimony, Oct. 31 Transcript, at 120:7-13, 122:15-123:20, 123:21-125:3, 127:23-128:15, 133:20-134:8, 135:13-135:25, 136:1-8, 138:3-139:21, 139:22-141:6, 143:5-144:5; P. Exh. 54, at 0088, 0091, 0376; P. Exh. 25, at 0003.

198. There are fees associated with all of the affirmative defenses and verification services identified in COPA, as well as all other services that claim to provide age verification. These fees apply any time a user attempts to access material on a Web site, even if there is no purchase. The fees must either be paid by the Web site or passed on to the users. As a result, Web sites such as Plaintiffs' sites, which desire to provide free distribution of their information, will be prevented from doing so. Russo Testimony, Oct. 25 Transcript, at 162:17-163:7, 166:1-13; P. Exh. 25, at 0024, 0033; P. Exh. 106, at 0015; Thaler Testimony, Nov. 1 Transcript, at 115:25-116:15, 116:16-117:8, 117:9-118:2; Cadwell Testimony, Oct. 31 Transcript, at 183:2-184:22, 192:7-193:1; Meiser Testimony, Oct. 31 Transcript, at 146:23-147:17; P. Exh. 6, at 0025; P. Exh. 54, at 0093; P. Exh. 106, at 0005, 0015; Peckham Testimony, Oct. 31 Transcript, at 55:22-25 (Urban Dictionary's mission is to provide content for free); Corinna Testimony, Nov. 2 Transcript, at 104:13-16 (Heather Corinna wishes to provide content for free); Griscom Testimony, Oct. 23 Transcript, at 84:25-85:13 (Nerve wants to reach widest audience possible).

199. Because of the nature of the Web, COPA would compel Web sites like Plaintiffs' which have interactive fora, such as discussion groups or chat rooms, to require users to pass through an age verification screen before entering any part of the interactive discussion – even if the vast majority of the speech in the interactive forum is not harmful to minors. There is no method by which the creators of an interactive forum could block access only to user-generated material that is "harmful to minors," but allow access to the remaining content. Walsh Testimony, Oct. 23 Transcript, at 129:2-13;

Peckham Testimony, Oct. 31 Transcript, at 47:9-48:6; P. Exh. 6, at 0025; P. Exh. 54, at 0370.

200. Because of the way search engines work, credit card or other COPA screens will prevent Web pages from being identified by search engines and, in turn, seen by users. As a result, search engines will be significantly affected by widespread use of verification screens and the placement of material behind such screens. The ultimate losers will be the millions of Internet users who rely on search engines for quick and accurate information, and the Web sites that depend on search engines to enable users to locate their sites. Felten Testimony, Oct. 25 Transcript, at 31:14-32:4; P. Exh. 54, at 0370.

201. Because COPA covers such a broad range of material, Web sites would need to create an organizational policy for determining what content must be placed behind an age verification screen. To comply with COPA, a Web site would need to apportion some of its staff, or to hire new staff members, to review both old and new content. Those individuals must somehow be able to apply the statute's definition of "harmful to minors," and have the authority and ability to decide whether to place content into an "adult section" behind the COPA screen. While it is theoretically possible for some Plaintiffs, analyzing all of the content on Web sites for COPA compliance would be an incredibly burdensome and impractical task given the vast quantity of speech available on many Web sites. Walsh Testimony, Oct. 23 Transcript, at 172:10-21; Peckham Testimony, Oct. 31 Transcript, at 47:12-25; Tepper Testimony, Oct. 30 Transcript, at 241:11-17; P. Exh. 54, at 0371-72, 0376.

202. For other Plaintiffs, the task would be impossible given that virtually all of the speech on their Web sites concerns subjects that by their nature involve frank and sexually explicit speech. Tepper Testimony, Oct. 30 Transcript, at 241:11-17; Griscom Testimony, Oct. 23 Transcript, at 90:16-21 (Nerve could attempt to segregate sexually explicit content, but because most content is explicit, "there would not be much left"); Glickman Testimony, Oct. 30 Transcript, at 133:15-134:2.

203. Because of the sexually explicit nature of the content on their Web sites, many Web sites, including many of the Plaintiffs', would be forced to place a credit card or age verification screen on the initial, home page of their sites and/or on each individual page in order to ensure that no user could access any of the content on the site until passing through such a screen. Tepper Testimony, Oct. 30 Transcript, at 241:18-242:7; Peckham Testimony, Oct. 31 Transcript, at 48:1-6.

204. The majority of Web users already refuse to register or provide any real personal information to Web sites if they have any alternative. Age verification is costly and difficult to use. Because requiring age verification would lead to a significant loss of users, content providers will have to either self-censor, risk prosecution, or shoulder the large burden of age verification. Russo Testimony, Oct. 25 Transcript, at 146:14-148:16; Griscom Testimony, Oct. 23 Transcript, at 88:8-20; Walsh Testimony, Oct. 23 Transcript, at 161:25-162:11; 163:4-11; 170:7-11; 173:10-20; Glickman Testimony, Oct. 30 Transcript, at 135:14-136:4; Lewis Testimony, Oct. 31 Transcript, at 110:4-13.

B. Access Restrictions Required by COPA's Affirmative Defenses Chill Speech While Failing to Protect Minors.

205. Because the vast majority of content on the Web is available for free, most Web users will not provide credit cards or personal information simply to access a Web

site. Walsh Testimony, Oct. 23 Transcript, at 171:5-172:9; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; Peckham Testimony, Oct. 31 Transcript, at 51:15-53:13; A. Smith Testimony, Oct. 26 Transcript, at 188:24-189:10; DeGenevieve Testimony, Nov. 1 Transcript, at 27:5-15; Snellen Testimony, Nov. 2 Transcript, at 136:2-12; S. Smith Testimony, Nov. 15 Transcript, at 116:4-6, 117:18-24.

206. Requiring users to provide a credit card or personal information before they can browse a Web page to determine what it offers will deter most users from ever accessing those pages, causing the traffic to Web sites such as Plaintiffs' to fall precipitously. Walsh Testimony, Oct. 23 Transcript, at 161:25-162:11, 163:4-164:2, 170:7-11, 171:15-172:9, 173:10-20; Glickman Testimony, Oct. 30 Transcript, at 134:6-136; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; A. Smith Testimony, Oct. 26 Transcript, at 188:24-189:10; Snellen Testimony, Nov. 2 Transcript, at 136:2-12; Clark Testimony, Nov. 14 Transcript, at 242:13-16; S. Smith Testimony, Nov. 15 Transcript, at 116:4-6, 117:18-24.

207. Requiring users to go through an age verification process would lead to a distinct loss in personal privacy. Many people wish to browse and access material privately and anonymously. Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. For example, people seeking sexual health information or information about sexuality issues generally, such as "Am I gay," or "is it normal to enjoy" certain sexual acts, will not seek out such information if it cannot be done confidentially and anonymously. The Sexual Health Network's experience demonstrates that many of the people who post questions to the Web site about sexual health or

sexuality issues have not previously asked anyone else, including their physician or even their sexual partner, for that information because they are too embarrassed or ashamed to do so non-anonymously. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired and, often, necessary information. Web sites such as Plaintiffs' will be deprived of the ability to provide this information to those users. Walsh Testimony, Oct. 23 Transcript, at 170:17-171:4; Tepper Testimony, Oct. 30 Transcript, at 178:7-23, 190:14-191:5, 212:1-10, 236:22-237:5, 238:9-239:17; Corinna Testimony, Nov. 2 Transcript, at 103:23-104:12 (anonymity is particularly important to women seeking information about sexuality); A. Smith Testimony, Oct. 26 Transcript, at 188:24-189:10; Snellen Testimony, Nov. 2 Transcript, at 139:18-141:8, 156:8-17; Griscom Testimony, Oct. 23 Transcript, at 88:8-20, 89:25-90:2; Smith Testimony, Oct. 26 Transcript at 188:24-10; P. Exh. 54, at 0372.

208. For example, Nerve has approximately 20,000 premium subscribers. Griscom Testimony, Oct. 23 Transcript, at 66:3-4. In all, less than one percent of Nerve's visitors are premium subscribers. *Id.* 66:5-17.

209. Nerve could not function as a premium-only site or a site that required everyone to pass through a verification screen. Griscom Testimony, Oct. 23 Transcript, at 84:15-85:14. A screen in front of Nerve's content would "cut our traffic down to close to zero." *Id.* at 86:19-24.

210. Even if Nerve's business could function with a credit card entrance barrier, Nerve would not want to operate with its content behind a screen, because it

could not reach as large an audience. Griscom Testimony, Oct. 23 Transcript, at 85:9-14.

211. When Nerve inserts any delay into accessing its content, traffic drops off. Griscom Testimony, Oct. 23 Transcript, at 87:11-18, 88:17-20.

212. Nerve's readers are concerned about their anonymity. Griscom Testimony, Oct. 23 Transcript, at 89:25-90:2.

213. Requiring users to provide Payment card or personal information to access the content on its Web site would dramatically deter users from accessing the Sexual Health Network's Web site, and prevent the Sexual Health Network from communicating with the very people it seeks to help. Tepper Testimony, Oct. 30 Transcript, at 178:7-23, 190:14-191:5, 212:1-10, 236:22-237:5, 237:25-239:17.

214. People seeking information about the sexual health and sexuality issues that the Sexual Health Network provides are extremely concerned about doing so anonymously because of the sensitive, potentially embarrassing, and distressing subject matters involved in sexual health and sexuality issues, so much so that many of the people coming to the site have not been willing to ask their questions to anyone else, including their personal physicians or their sex partners. Understanding this, the Sexual Health Network does everything possible to make it easy for its users to access the content on its site. Tepper Testimony, Oct. 30 Transcript, at 178:7-23, 190:14-191:5, 212:1-10, 236:22-237:5, 237:25-239:17.

215. If it were required to install a payment card or age verification screen on its site, the Sexual Health Network would have to place that screen before anyone could access any of the content on its Web site. In other words, the Sexual Health Network

would likely have to install such a screen on the home page and/or on every single Web page to ensure that users could not access any page before passing through the verification screen. Tepper Testimony, Oct. 30 Transcript, at 241:11-17.

216. The Sexual Health Network would likely have to shut its Web site down if it were required to force its users to provide a credit card or other personal information to access the site. Tepper Testimony, Oct. 30 Transcript, at 242:8-19.

217. If COPA were to take effect and urbandictionary.com were to implement the credit card affirmative defense, the payment card screen would have to appear at the entrance to the website. That is because it would not be possible for urbandictionary.com to segregate its sexually explicit content from its non-sexually explicit content, for two reasons. First, with one million definitions on the site, there is simply too much content to be identified and sorted. Second, Aaron Peckham has no clear definition of what constitutes sexually explicit content, and even if he were to attempt to segregate his content, he might draw the line in a different place than would his volunteer editors and users. Peckham Testimony, Oct. 31 Transcript, 47:9 to 48:6.

218. A payment card screen in front of the content on scarleteen.com would preclude the site from reaching much of its intended audience of minors and young adults. Corinna Testimony, Nov. 2 Transcript, at 102:25-103:6.

219. There are women who place a premium on being able to access speech on the Internet anonymously, especially when that speech is about sex. Corinna Testimony, Nov. 2 Transcript, at 104:2-12.

220. Before visitors to www.condomania.com enter a section of the Web site called “After Hours,” which contains sex toys such as dildos and vibrators more sexually

explicit than products in other areas of the site, they encounter a "splash page" which advises them of the adult nature of the products. This "splash page" deters between 15 percent and 20 percent of visitors from entering the "After Hours" section. Based on this experience, Condomania reasonably believes that placing an age verification screen on www.condomania.com would have a negative effect on its business and its ability to reach its intended audience. Glickman Testimony, Oct. 30 Transcript, at 126:10-15, 135:14-136:4.

221. The Leslie/Lohman Web site does not charge a fee to visitors, or require any personal information before entering the Web site, for fear that it would deter more people than it would attract. Snellen Testimony, Nov. 2 Transcript, at 135:25-140:4, 142:22-24, 143:15-23.

222. Anonymity is important to individuals who seek to view or purchase sexually explicit gay and lesbian art. Snellen Testimony, Nov. 2 Transcript, at 139:18-140:20.

223. Anonymity is particularly important for older minors searching for their sexual identity. The availability of the Leslie/Lohman Web site lets these older minors know they are not alone, and they are not perverts or abnormal. Snellen Testimony, Nov. 2 Transcript, at 140:21-141:8, 156:8-17.

224. It would be extremely harmful to Ms. Smith's career, to her record sales, and to the impact she is trying to have if she were forced to require visitors to her Web site to provide payment card information just to access her site. The only way an up-and-coming artist like herself, especially someone who is not in the mainstream, can attract new fans and listeners is by making her songs freely and easily available on the

Web to a worldwide audience. In addition, a payment card requirement would make it impossible for Ms. Smith to reach many of the people to whom she is trying to convey her message of hope and positivity, both because many of her listeners do not have payment cards and because many will not be willing to provide such personal information just to hear her music. A. Smith Testimony, Oct. 26 Transcript, at 195:3-21, 217:1-218:1-14.

225. Requiring users to provide a payment card or personal information before they can browse a Web page will also cause many users to leave the Web site because Internet users do not like being forced to register or to provide any information just to access content on the Web. Walsh Testimony, Oct. 23 Transcript, at 164:20-165:16; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17.

226. The evidence in the record actually shows that many Internet users will not be willing to register or subscribe to Web sites such as Plaintiffs' sites simply to access content on the sites, and that if a Web site started to require users to register before accessing the site, the site would receive fewer visitors. Walsh Testimony, Oct. 23 Transcript, at 161:25-162:11; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; S. Smith Testimony, Nov. 15 Transcript, at 172:13-16.

227. As one example, in the years following the dot-com bust (2001-2003), Salon experimented with switching from a free, non-subscription Web site to a subscription-based Web site. Salon experienced a serious loss of traffic as a result of that switch. Whereas a popular cover story on Salon previously received approximately 100,000 page views, under the subscription model, the same sort of story received

approximately 6,000-7,000 page views. Walsh Testimony, Oct. 23 Transcript, at 161:25-162:11, 163:4-164:2.

228. Even among those users who are willing to register to access material on certain Web sites, many will not be willing to provide real personal information, such as their actual name, address, or telephone number. The vast majority of Web sites that presently require some form of registration do not require users to provide real names or any other personally identifiable information. Tepper Testimony, Oct. 30 Transcript, at 193:25-194:8; S. Smith Testimony, Nov. 15 Transcript, at 172:24-173:14; Peckham Testimony, Oct. 31 Transcript, at 52:15-53:13 (describing bugmenot.com, a site that permits users to share passwords so as to avoid providing personal information).

229. Imposing any barriers on access to a Web site, even barriers that do not require Internet users to provide their payment card information or other personal information, will severely decrease the number of users who access a Web site. Walsh Testimony, Oct. 23 Transcript, at 165:17-166:6; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17.

230. As one example, Salon's "site pass," which requires users to view a short, 10-30 second advertisement prior to being given free access to the requested content, causes Salon to lose 40 to 90 percent of its traffic, because those users are not willing to put up with that access barrier. Walsh Testimony, Oct. 23 Transcript, at 165:17-166:6.

231. COPA's requirement that Web sites maintain the confidentiality of information submitted for purposes of age verification would not alleviate the deterrent effect of age verification on users, because users must still disclose the personal information to a Web site to pass through the screen, and then rely on these entities,

many of whom are unknown and have no actual person identified with them, to comply with the confidentiality requirement. Tepper Testimony, Oct. 30 Transcript, at 178:7-23, 190:14-191:5, 212:1-10, 236:22-237:5, 238:9-239:17; P. Exh. 6, at 25 (noting that the "[c]ollection of individually-identifiable information at central points via this system poses privacy risks").

232. COPA does not provide any recourse to users for confidentiality violations by Web sites. In fact, COPA explicitly grants immunity to content providers for any action taken to comply with COPA. 47 U.S.C. § 231(c)(2).

233. United States Web sites will suffer and be put at a distinct disadvantage because foreign Web sites will not have to comply with COPA. Most likely, the vast majority of non-U.S. Web sites will ignore COPA. As a result, many users, inside and outside the U.S., will gravitate toward non-U.S. sites that offer the same or similar information and services as U.S. Web sites, but that do not require the users to pass through an age verification screen. Walsh Testimony, Oct. 23 Transcript, at 171:15-172:9; P. Exh. 25 at 0037-0039; P. Exh. 54, at 0235; P. Exh. 106.

234. Plaintiffs would not be able to survive financially and continue providing their speech if they were forced to become premium-only Web sites where the content is accessible only to members who provide their credit card or other personal information because of the loss of traffic that would occur. Walsh Testimony, Oct. 23 Transcript, at 159:3-21, 161:25-162:11, 168:15-20**;** Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; Griscom Testimony, Oct. 23 Transcript, at 84:9-24.

235. Requiring Plaintiffs to become members-only Web sites would also greatly affect Plaintiffs' missions for why they communicate on the Web in the first

place. Walsh Testimony, Oct. 23 Transcript, at 168:21-169:11; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17; Griscom Testimony, Oct 23 Transcript, at 84:25-85:13.

1. Defendant's Experts' Opinions are Largely Unsupported, but to the Extent they are Supported, they Confirm That Users Will be Deterred by COPA's Affirmative Defenses.

236. Requiring Internet users to provide payment card information or other personally identifiable information to access a Web site would significantly deter many users from entering the site, because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet. S. Smith Testimony, Nov. 15 Transcript, at 116:4-6, 117:18-24.

237. Although the Internet has become much more familiar to most people, numerous studies show that Internet users today are increasingly concerned about identity theft and fraud on the Internet and that their fears have grown, not decreased, over time. S. Smith Testimony, Nov. 15 Transcript, at 119:11-15.

238. Consumer Reports Web Watch issued a report on Internet users' security concerns on October 26, 2005. The report was based on a survey conducted by Princeton Survey Research Associates International. Princeton Survey Research provides reliable sources of information. S. Smith Testimony, Nov. 15 Transcript, at 119:20-120:12.

239. The October 26, 2005 Consumer Reports study found that nine out of ten U.S. Internet users over 18 years old have made changes to their behavior due to fear of identity theft. The study also found that of those changes made because of fear of identity theft, 30 percent of people reported that they had reduced their overall use of the Internet, that 25 percent said that they stopped buying things online, and that of those

people who do make purchases online, 29 percent have cut back on how often they buy things online. S. Smith Testimony, Nov. 15 Transcript, at 120:13-121:16.

240. The Consumer Reports study also found that 88 percent of the people surveyed said that keeping personal information safe and secure is very important for a Web site they visit, and that for all online users, concern about identity theft is substantial and a worry that has changed their behavior in sweeping ways. More specifically, because of their concerns, a majority of Internet users (53 percent) have stopped giving out personal information on the Internet. S. Smith Testimony, Nov. 15 Transcript, at 121:25-122:17, 124:14-18.

241. The Javelin company issued a report on identity fraud in 2005 that Professor Smith cited in his rebuttal expert report. Javelin is a reliable source of information. The Javelin study similarly found that there are growing fears today about identity theft on the Internet. S. Smith Testimony, Nov. 15 Transcript, at 124:19-125:5.

242. Forrester Research issued a report on April 10, 2006 entitled "Online Retailers Face a Tough Road Ahead, Waning Customer Satisfaction Forces Retailers to Form Loyalty and Trust." Forrester Research is a reliable source of information and is widely used in the industry. The Forrester Research report found that overall satisfaction with e-commerce shopping experiences and credit card security trust is declining, that credit card security concerns have intensified, and that whether founded on reality or not, all online shoppers, even experienced buyers, worry about credit card security. S. Smith Testimony, Nov. 15 Transcript, at 125:6-128:13.

243. Recent publicity about thefts of personal information on the Internet has heightened Internet users' concerns. S. Smith Testimony, Nov. 15 Transcript, at 129:22-130:2.

244. Defendant's expert, Professor Smith, did not mention these recent studies from reliable organizations on the subject of Internet users' concerns about security on the Internet in his expert report. S. Smith Testimony, Nov. 15 Transcript, at 131:1-5.

245. Professor Smith did not cite any statistics or data in his expert report that indicated that Internet users' concerns about security on the Internet were decreasing. S. Smith Testimony, Nov. 15 Transcript, at 118:17-20.

246. Some Internet users are reluctant to provide personal information or credit card information over the Internet. S. Smith Testimony, Nov. 15 Transcript, at 138:4-8, 143:20-22; Walsh Testimony, Oct. 23 Transcript, at 171:15-172:9.

247. Although Defendant's expert, Professor Smith, contends in his expert report that subscription-based and registration-based Web sites are of increasing importance on the Web, Professor Smith does not know what percentage of sites require registration or subscription, and he has no idea if that figure is even higher than 5 percent of all Web sites. In fact, Professor Smith does not cite to any studies, statistics, or data of any kind indicating that subscription or registration models are prevalent or common on the Web. S. Smith Testimony, Nov. 15 Transcript, at 169:17-22, 172:9-12; D. Exh. 91.

248. Professor Smith conceded that there are no studies or data in his expert report that stand for the proposition that Internet users will be willing to register or subscribe to Web sites such as Plaintiffs' sites simply to access free content on the Web.

In fact, Professor Smith is not aware of any research, studies, or other evidence concerning the impact on a Web site's traffic if the site were to switch to a subscription model. S. Smith Testimony, Nov. 15 Transcript, at 171:1-10, 172:17-23.

249. Professor Smith similarly does not know what the impact on traffic to Salon's Web site was when they experimented with a subscription model or what the impact has been for Nerve or Heather Corinna's Web sites. S. Smith Testimony, Nov. 15 Transcript, at 170:13-25.

250. Defendant's expert Professor Smith has decided not to enter Web sites because they require registration or a subscription. S. Smith Testimony, Nov. 15 Transcript, at 171:15-17, 174:20-22.

251. According to Defendant's other expert, Mr. Clark, requiring the use of a payment card to access a Web site is likely to reduce the number of Web site visitors. Clark Testimony, Nov. 14 Transcript, at 242:13-16. It is also Mr. Clark's opinion that forcing Salon to require its users to provide payment card information to access the site would likely reduce the number of visitors to the Salon Web site and could negatively impact Salon's advertising revenue. Clark Testimony, Nov. 14 Transcript, at 243:8-19.

252. Many people are still not willing to purchase anything on the Internet, and there are some Internet users who will not use a credit card online for any purpose. At least 20 percent of people in the United States do not purchase anything online. S. Smith Testimony, Nov. 15 Transcript, at 142:15-20, 145:11-14, 145:22-24.

253. It is the opinion of Mr. Clark that one third of customers do not feel comfortable using credit cards to shop online, and that 50 percent of consumers do not feel comfortable using debit cards to shop online. Mr. Clark does not know how many

customers are comfortable using debit cards or credit cards to shop online simply to access content. Clark Testimony, Nov. 14 Transcript, at 241:6-21.

254. Even if a Web site utilizes the greatest security measures possible, there will be some Internet users who will be deterred from accessing Web sites by having to provide a credit card number. S. Smith Testimony, Nov. 15 Transcript, at 132:14-18.

255. No matter what security steps a Web site takes, if a Web site asks a user for their credit card information prior to the final check-out step in a purchase process, the site risks losing the customer. Amazon.com, for example, does not ask for a user's credit card when he or she first enters the Web site, is searching for products, or finds a product and puts it into the shopping cart. Instead, Amazon.com waits until the very last step, the checkout step, to ask for the credit card. S. Smith Testimony, Nov. 15 Transcript, at 147:13-148:12.

256. Although some Internet users may risk transmitting their credit card or personal information over the Internet when they are making a purchase, many users will not provide that information just to browse on a Web site, particularly if that content is available on another Web site that does not require entry of that information. S. Smith Testimony, Nov. 15 Transcript, at 140:16-19; Walsh Testimony, Oct. 23 Transcript, at 171:15-172:9; Tepper Testimony, Oct. 30 Transcript, at 238:9-239:17.

257. If the same content is available on two different Web sites, and one site requires use of a credit card number just to look at the site, and the second site does not, Internet users will go to the site that does not require input of the credit card information. S. Smith Testimony, Nov. 15 Transcript, at 131:15-132:13.

258. Someone who is not interested in purchasing anything on a Web site will be less likely to overcome a barrier to access a Web page than someone who wants to purchase something. S. Smith Testimony, Nov. 15 Transcript, at 137:24-138:3.

259. Defendant's expert, Professor Smith, was the author of a study published in July 2003 entitled, "Why People Don't Shop Online: A Lifestyle Study of the Internet Consumer." The study concluded that a substantial reason why people do not shop on the Internet is because of fear. More specifically, the study found that over 70 percent of those people who did not shop online agreed with the statement that, "I don't want to give a computer my credit card number," and that even a third of the people who do shop online also agreed with that statement. The study also found that three-quarters of the people who do not shop online, and nearly half of the people who shop online, worry about having their credit card number stolen on the Internet. The findings in this study were consistent with studies that had previously been conducted, which similarly concluded that credit card concern was the most important deterrent to online shopping. S. Smith Testimony, Nov. 15 Transcript, at 151:1-154:25.

260. The findings in Professor Smith's study contradict Professor Smith's opinion in this case that Internet users would not be significantly affected by having to provide credit card information to access free content on Web sites were COPA to go into effect. S. Smith Testimony, Nov. 15 Transcript, at 151:1-155:10.

261. Professor Smith relied on his July 2003 study to publish a subsequent article in the October 2003 issue of BYU's School of Management Business magazine. S. Smith Testimony, Nov. 15 Transcript, at 155:15-25.

262. Another study by Professor Smith was published in the International Business and Economic Research Journal in April 2004. This study relied on the data from the earlier study, and expressly stated that the earlier study "forms a springboard for the testing of the subsequent hypothesis." In this April 2004 study, Professor Smith did not change any of the conclusions or recommendations from his earlier study. S. Smith Testimony, Nov. 15 Transcript, at 156:2-24.

263. In 2005, Professor Smith published another journal article based on his July 2003 study about why people do not shop on the Internet. That 2005 article also relied on the same data from the earlier study. S. Smith Testimony, Nov. 15 Transcript, at 158:6-23.

264. Professor Smith recently published a study entitled "E-Shopping Lovers and Fearful Conservatives, A Market Segmentation Analysis." That study was published in a well-respected journal in the summer of 2006, after Professor Smith wrote his expert report and prepared his expert opinion in connection with this case. This study was based on new research that Professor Smith conducted. S. Smith Testimony, Nov. 15 Transcript, at 158:24-160:13.

265. The findings in Professor Smith's 2006 study contradict Professor Smith's opinion in this case. His study concluded that there are still Internet users who resist online shopping even though they engage in other online activities, and that their security fears typically inhibit these users from engaging in electronic exchange. More specifically, the study found that 48 percent of the people who do not shop online agreed with the statement that, "I don't want to give a computer my credit card number," and that 26 percent of online shoppers agreed with that statement. The study also found that

61 percent of the non-shoppers and 47 percent of the online shoppers agreed with the statement that, "I worry about my credit card number being stolen on the Internet." S. Smith Testimony, Nov. 15 Transcript, at 160:14-161:10, 163:21-165:7.

266. Although this study was published in a peer reviewed journal in the summer of 2006 (well after he prepared and wrote his expert report), in his trial testimony, Professor Smith attempted to avoid the inconsistencies with his opinion in this case by indicating that the study's data was not very recent. Professor Smith did not mention or cite any data in his expert report on Internet users' willingness to provide credit card information to Web sites that is more recent than the data discussed in his 2006 study in his expert report in this case. S. Smith Testimony, Nov. 15 Transcript, at 166:11-167:3.

267. In his expert report in this case, Professor Smith did not mention, cite, or even consider this 2006 study or any of his other studies that he had personally conducted regarding Internet users' fears and their non-willingness to provide their credit card information to Web sites. D. Exh. 91.

268. Although Professor Smith attempted to downplay his own prior research by stating that it merely reflected Internet users' attitudinal beliefs, Professor Smith conceded that there are valuable insights for Web sites to learn by examining Internet users' attitudinal beliefs, and that he would make recommendations to Web sites based on users' attitudinal beliefs. S. Smith Testimony, Nov. 15 Transcript, at 155:1-9.

269. Professor Smith also attempted to avoid his own research by claiming at trial that certain unidentified "statistics" show that despite people's feelings and fears, people are buying things online. Professor Smith did not cite any data or statistics

concerning how many Internet users are shopping on the Internet in his expert report. S. Smith Testimony, Nov. 15 Transcript, at 134:2-8.

270. Professor Smith opined that COPA would not have a significant impact on commercial Web sites or Internet users. Professor Smith did not cite any data or statistics, and expressed no opinion, as to how many potential purchasers would be deterred by having to pass through a COPA verification screen to access the Web sites covered by COPA. S. Smith Testimony, Nov. 15 Transcript, at 135:24-136:8.

271. One of the assumptions underlying Professor Smith's opinion about the impact of COPA is that COPA covers only Web sites with "pornographic material." S. Smith Testimony, Nov. 15 Transcript, at 167:4-10.

272. One of the assumptions underlying Professor Smith's opinion about the impact of COPA is that the only Web sites that are covered are those where purchases are made, and ignores the extremely prevalent advertising-based business model. S. Smith Testimony, Nov. 15 Transcript, at 168:5-169:8.

273. Professor Smith was deposed after he had completed his expert report and had prepared his expert opinion. At the time of his deposition, Professor Smith stated that he had no opinion as to the impact of COPA on any of the Plaintiffs in this case. S. Smith Testimony, Nov. 15 Transcript, at 108:3-5.

274. At trial, Professor Smith asserted that he now had reached an opinion as to the impact of COPA on three of the Plaintiffs, Nerve, Salon, and the Sexual Health Network. Professor Smith still has no opinion about the impact of COPA on any of the other Plaintiffs. S. Smith Testimony, Nov. 15 Transcript, at 111:13-18.

275. It is not Professor Smith's opinion that COPA will have no impact on commercial Web sites. Professor Smith conceded that COPA will have an impact on commercial Web sites. According to Professor Smith, there will only be a small impact and a small financial cost to commercial Web sites. S. Smith Testimony, Nov. 15 Transcript, at 112:25-11.

276. Professor Smith's opinion that the impact of COPA on commercial Web sites will not be significant is based on his assumption that Web sites will not have to place an age verification screen on their home page. S. Smith Testimony, Nov. 15 Transcript, at 113:12-21.

277. Professor Smith conceded that his opinion would change as to the amount of impact that COPA would have on Web sites if the sites had to place verification screens on their home page. S. Smith Testimony, Nov. 15 Transcript, at 114:3-7.

278. It is Professor Smith's opinion that the operator of any Web site, including those with pornographic material, should never require age verification on the first page of the site because it is preferable to first bring people into the site, to let them look around and see what is in the site before requiring the viewer to pass through the verification. It would, accordingly, be bad for business and would impose a substantial burden on Web sites if they were forced to place an age verification screen before users could enter the site and see what was there. S. Smith Testimony, Nov. 15 Transcript, at 179:15-180:6.

279. Professor Smith's opinion about the impact of COPA is based on his assumption that quality content is more valued than free content. Professor Smith does

not cite to any studies to support that assertion. S. Smith Testimony, Nov. 15 Transcript, at 174:23-175:5.

280. Prior to being retained by Defendant, Professor Smith had never studied the motivations of Internet users seeking out pornographic material. S. Smith Testimony, Nov. 15 Transcript, at 175:6-176:4.

281. In his expert report, Professor Smith discusses one psychology journal article regarding the motivations of individuals seeking out pornography. D. Exh. 91, at 14. Professor Smith does not personally know the author of that article, has never talked to him, does not know if he is well-respected in the field, and does not know if his work is particularly controversial in the field. S. Smith Testimony, Nov. 15 Transcript, at 175:13-177:25.

C. Payment Cards are Not an Effective Method of Verifying Age.

1. In General.

282. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a credit card or debit account. 47 U.S.C. § 231 (c) (1).

283. This affirmative defense presumes that adults, but not many minors, have credit cards, debit cards, or prepaid cards. P. Exh. 6, at 0025-0026; P. Exh. 25, at 0023-0024; P. Exh. 54, at 0092.

284. The terms "debit account" and "account" include debit cards, reloadable prepaid cards, and non-reloadable prepaid cards with the Visa or MasterCard logo. Payment cards with the Visa and MasterCard logo can be used to make purchases on the Internet. Mann Testimony, Nov. 6 Transcript, at 68:10-69:16; 80:7-81:8; 82:8-83-7; Clark Testimony, Nov. 14 Transcript 207:13-212:10.

285. There are no laws preventing children from obtaining payment cards, including credit cards, debit cards, and prepaid cards, in their own name. Mann Testimony, Nov. 6 Transcript, at 144:9-145:20; P. Exh. 139, at 0003; P. Exh. 141, at 0001.

286. Payment card associations prohibit Web sites from claiming that use of a payment card is an effective method of verifying age, and prohibit Web sites from using credit or debit cards to verify age. Russo Testimony, Oct. 25 Transcript, at 72:23-73:8; Cadwell Testimony, Oct. 31 Transcript at 185:15-186:11, 187:3-187:23; Thaler Testimony, Nov. 1 Transcript, at 111:20-113:20; Bergman Testimony, Nov. 7 Transcript at 16:4-17:17, 18:21-19:25; P. Exh. 106, at 0004; P. Exh. 139 at 0003-0004; P. Exh. 141, at 0001.

287. Payment card associations advise consumers not to offer payment cards to merchants as a proxy for age. Russo Testimony, Oct. 25 Transcript, at 72:16-73:3; Bergman Testimony, Nov. 7 Transcript, at 16:4-17:17; P. Exh. 139 at 0003-0004.

288. Payment cards do not distinguish between cardholders who are minors and those who are adults. P. Exh. 54, at 0375; Peirez Testimony, Oct. 31 Transcript, at 251:15-20; Bergman Testimony, Nov. 7 Transcript, at 4:3-6:2.

2. Minors Have Access to Payment Cards.

289. Payment card issuers today increasingly market credit cards, debit cards, and prepaid cards to minors as young as 13. The youth market presents "dramatic revenue generating opportunities." Currently, one of the main thrusts of credit card marketing in this country is to get payment cards into the hands of the "coveted youth segment" as early as possible. This marketing focus is still rather new, and in the

coming years, it is likely that this focus will result in more and more minors having payment cards. Visa's "Visa Buxx" card is one example of a payment card that is specifically designed to be used by minors. Mann Testimony, Nov. 6 Transcript, at 75:18-77:2, 85:14-86:11; Bergman Testimony, Nov. 7 Transcript at 4:3-6:2, 21:16-23:19, 46:20-47:25; P. Exh. 25, at 0023-0024; P. Exh. 34, at 0006-0007; P. Exh. 54, at 0371, 0377; P. Exh. 148, at 0002, 0004.

290. Many children have access to credit or debit cards. A significant percentage of minors have access to credit or debit cards with the express permission of their parents. A significant percentage of minors also have access to credit or debit cards without the knowledge or consent of their parents. Russo Testimony, Oct. 25 Transcript, at 228:13-17; Glickman Testimony, Oct. 30 Transcript, at 102:12-103:1; Peirez Testimony, Oct. 31 Transcript at 240:7-24, 251:15-20; Mann Testimony, Nov. 6 Transcript, at 86:12-17, 96:18-97:14, 114:17-24; Rinchiuso Testimony, Nov. 6 Transcript, at 237:23-238:12; Bergman Testimony, Nov. 7 Transcript, at 4:3-6:2, 6:3-7:25, 8:1-7; 8:8-9:22; 13:23-15:13; P. Exh. 17, at 0002, 0007; P. Exh. 34, at 0003-0008; P. Exh. 54, at 93; P. Exh. 93, at 0010; P. Exh. 139, at 0003-04.

291. Defendant's expert, Mr. Clark, concedes that payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards. Clark Testimony, Nov. 14 Transcript, at 179:20-180:6.

292. Minors have access to reloadable prepaid cards. Russo Testimony, Oct. 25 Transcript, at 229:2-6; Mann Testimony, Nov. 6 Transcript, at 133:5-134:21; Bergman Testimony, Nov. 7 Transcript, at 4:3-6:2, 21:16-23:19; P. Exh. 17, at 0002, 0007; P. Exh. 25, at 0023-0004; P. Exh. 34, at 0006-0007; P. Exh. 54, at 0093.

293. Many employers, such as McDonalds, pay employees, including minors, by providing reloadable prepaid cards. Mann Testimony, Nov. 6 Transcript, at 70:2-19; D. Exh. 93, at 0021.

294. There is no evidence in the record that payment card issuers will not issue reloadable prepaid cards to minors. Clark Testimony, Nov. 14 Transcript, at 126:25-130:19.

295. Minors have access to non-reloadable prepaid cards. P. Exh. 17, at 0002, 0007; P. Exh. 25, at 0023-0024; P. Exh. 34, at 0006-0007; Bergman Testimony, Nov. 7 Transcript, at 4:3-6:2.

296. There are millions of prepaid cards in circulation. Bergman Testimony, Nov. 7 Transcript, at 26:13-27:4

297. There is no reason for a vendor of prepaid cards to decline selling non-reloadable prepaid cards to minors. P. Exh. 54, at 0371; D. Exh. 93, at 0021.

298. Condomania sells its products, both online and in its New York store, to persons 17 years old and younger. Many of these young customers use payment cards to make purchases. These teenagers comprise an important part of www.condomania.com's intended audience. Glickman Testimony, Oct. 30 Transcript, at 100:17-103:1, 107:16-108:10.

299. The best estimate is that at least half of all minors have access to credit cards, debit cards, or prepaid cards. The percentage of 16 year-olds with access to payment cards is significantly higher than the percentage of 12 year-olds with access to such cards. Mann Testimony, Nov. 6 Transcript, at 86:12-17, 96:18-97:14, 114:17-24; P. Exh. 17, at 0002, 0007; P. Exh. 34, at 0003-0008; P. Exh. 93, at 0010.

300. It is the opinion of Mr. Clark that 11 percent of minors age 12 to 17 have credit cards, debit cards, or reloadable prepaid cards in their own name. Based on information from the U.S. Census, Mr. Clark calculated that this 11 percent corresponds to 2.8 million minors age 12 to 17 that have credit cards, debit cards or reloadable prepaid cards in their own name. Clark Testimony, Nov. 14 Transcript, at 180:13-16, 186:11-22.

301. At the time of his report, Mr. Clark based his opinion that 11 percent of minors age 12 to 17 have credit cards, debit cards or reloadable prepaid cards in their own name exclusively on one telephone conversation with an employee of a company called Teenage Research Unlimited. Mr. Clark did not ask this employee whether the Teenage Research Unlimited information included information about reloadable prepaid cards. Clark Testimony, Nov. 14 Transcript, at 188:15-190:5.

302. At the time of his report, Mr. Clark did not know how many minors had reloadable prepaid cards. Clark Testimony, Nov. 14 Transcript, at 194:22-195:2.

303. Mr. Clark admitted that his estimate that 11 percent of minors age 12 to 17 have credit cards, debit cards or reloadable prepaid cards in their own name is too low if minors have prepaid cards that are not included in the Teenage Research Unlimited data. The term "reloadable prepaid card" does not appear in the Teenage Research Unlimited research data. Clark Testimony, Nov. 14 Transcript, at 190:6-23, 191:5-23, 192:11-18, 193:8-13.

304. Mr. Clark believes that it is reasonable to double the number of minors with credit cards, debit cards, or reloadable prepaid cards in their own name in order to account for minors that may borrow such payment cards for their use on the Internet.

Mr. Clark has no experience or expertise in the payment card industry with respect to the number of minors that can borrow payment cards. Clark Testimony, Nov. 14 Transcript, at 181:19-182-4, 183:13-16.

305. At the time of his report, Mr. Clark did not know how many minors could borrow reloadable prepaid cards. Clark Testimony, Nov. 14 Transcript, at 195:3-6.

306. There is no evidence in the record that payment card issuers will only issue credit cards or debit cards to adults because of the "know your customer" requirements contained in the Patriot Act. Clark Testimony, Nov. 14 Transcript, at 120:4-125:20.

307. Payment card-based age verification schemes are not difficult to bypass. Minors can obtain passwords on the Internet to access "protected" Web pages. Minors can also circumvent password screens because URLs of "protected" Web pages can be shared. Russo Testimony, Oct. 25 Transcript, at 144:7-25, 158:8-160:3; Glickman Testimony, Oct. 30 Transcript, at 52:14-53:13; P. Exh. 25, at 0024, 0025.

308. Payment card statements for credit cards that were issued to a minor without the parents' consent will be sent to the minor, not to a parent. Clark Testimony, Nov. 14 Transcript 214:2-6.

309. Delay in issuing a payment card statement to parents means that unauthorized access to harmful to minors materials can occur. P. Exh. 6, at 0025.

310. Even if parents review payment card statements, either their own or those of cards issued with their permission to their children, they may not be able to identify transactions on sexually explicit Web sites because the adult nature of such transactions

is often not readily identifiable from information provided on the statement. Clark Testimony, Nov. 14 Transcript, at 214:7-10; P. Exh. 54, at 0093.

311. Payment card statements for reloadable prepaid cards that were issued to a minor in their own name will be sent to the minor, not to a parent. Clark Testimony, Nov. 14 Transcript 213:3-11.

312. There is no way for a merchant, such as a Web site, to know that a user is actually an adult. Merchants, including Web sites, that accept Visa or Mastercard credit cards and debit cards will honor all Visa or MasterCard payment cards, including reloadable and non-reloadable prepaid cards. Russo Testimony, Oct. 25 Transcript, at 120:6-11, 124:1-6, 157:3-158:8, 164:15-165:7; 166:14-167:12; Bergman Testimony, Nov. 7 Transcript at 6:3-7:25; 21:16-23:19; Thaler Testimony, Nov. 1 Transcript at 104:12-105:9, 105:10-106:25; Cadwell Testimony, Oct. 31 Transcript at 164:23-166:8, 178:24-181:22.

313. The minimum information required for processing a payment card transaction is payment card number and expiration date. Glickman Testimony, Oct. 30 Transcript, at 101:20-24; Cadwell Testimony, Oct. 31 Transcript, at 174:15-175:15, 178:4-20; Clark Testimony, Nov. 14 Transcript, at 202:7-205:3.

314. Merchants, including Web sites, that accept payment cards are not required to verify an address that may or may not be associated with a payment card. Cadwell Testimony, Oct. 31 Transcript, at 174:15-175:15, 178:4-20.

315. The payment card associations do not require Web site operators to decline non-reloadable prepaid cards. Mr. Clark testified that Web sites have the ability

to decline non-reloadable prepaid cards, not that they will actually do so. Clark Testimony, Nov. 14 Transcript, at 195:15-196:3, 197:8-11.

316. At the time of his report, Mr. Clark did not know what percentage of Web sites decline non-reloadable prepaid cards. Mr. Clark also did not know what percentage of payment processors for commercial adult sexual content Web sites, such as CCBill, will decline non-reloadable prepaid cards. Clark Testimony, Nov. 14 Transcript, at 196:4-9, 201:11-202:5.

3. A Payment Card Requirement Curtails the Ability of Web speakers to reach end users.

317. Many adults do not have credit or debit cards. Mann Testimony, Nov. 6 Transcript, at 151:18-152:16; Russo Testimony, Oct. 26 Transcript, at 7:12-14; P. Exh. 25 at 0024; P. Exh. 34, at 0011.

318. Many adults do not have reloadable prepaid cards. Mann Testimony, Nov. 6 Transcript, at 151:18-152:16; P. Exh. 34, at 0011.

319. Mr. Clark has no support for his assertion that adults without bank accounts or credit cards can make use of reloadable or non-reloadable prepaid cards. Clark Testimony, Nov. 14 Transcript, at 75:7-23.

320. Requiring use of a payment card to enter a site would impose a significant economic cost on Web entities. In addition to set-up fees and administrative fees, Web entities will also need to pay fees for processing payment card information for each transaction. Russo Testimony, Oct. 25 Transcript, at 162:17-163:7; Lewis Testimony, Oct. 31 Transcript, at 109:6-24; Cadwell Testimony, Oct. 31 Transcript at 183:2-184:22; Thaler Testimony, Nov. 1 Transcript at 116:13-117:8, 117:9-118:2, 118:3-119:7;

Corinna Testimony, Nov. 2 Transcript, at 104:17-105:7; Clark Testimony, Nov. 14 Transcript, at 239:12 – 240:15; P. Exh. 106, at 0005, 0015.

321. Financial institutions will not process or verify a payment card in the absence of a financial transaction. Express policies of the payment card associations prohibit online merchants who sell content from processing transactions in the amount of zero dollars ($0). Verification by payment card will therefore be practically infeasible for all of the Plaintiffs and most other Web site operators and content providers covered by COPA who distribute their content and material for free. Thaler Testimony, Nov. 1 Transcript at 118:8-16; Rinchiuso Testimony, Nov. 6 Transcript at 242:16-24; Clark Testimony, Nov. 14 Transcript, at 214:11-218:16; P. Exh. 6, at 0025; P. Exh. 34, at 0010; P. Exh. 54, at 0373.

322. The purpose of the payment card associations' processing systems is to process financial transactions or purchases. Those associations have regulations and policies designed to prevent their systems from being used for other, non-payment transaction-based purposes. Permitting zero-dollar transactions would threaten the system's capacity to process transactions, and would increase fraud by enabling criminals to enter numbers randomly into the system to identify active card numbers. Peirez Testimony, Oct. 31 Transcript at 245:25-246:8; Bergman Testimony, Nov. 7 at 27:5-30:3; P. Exh. 34, at 0010.

323. Mr. Clark concedes that the policies of Visa and MasterCard do not allow zero dollar transactions. Mr. Clark has no indication that the payment card associations are intending to change that policy. Clark Testimony, Nov. 14 Transcript, at 214:15-21.

324. Even if Visa and MasterCard were to change their policy to allow zero dollar transactions, Web sites would still have to pay processing fees for each transaction. Clark Testimony, Nov. 14 Transcript, at 215:7-14.

325. There are fees associated with online purchases which are subsequently canceled or denied by the payment card holder (chargeback fees). Chargeback fees are higher for Web entities that provide content that is associated with a higher risk of a denial of payment. The risk of chargebacks is higher for Web entities that provide controversial sexually explicit content. Russo Testimony, Oct. 25 Transcript, at 81:7-82:22, 163:11-165:25; Bergman Testimony, Nov. 7 Transcript at 25:10-23, 30:23-31:23; P. Exh. 106, at 0015.

326. Credit and verification charges must either be absorbed by the content provider or passed on to users. This cost will increase according to the number of visitors to a site. Many of the larger sites have well over a million unique visitors per day. Russo Testimony, Oct. 25 Transcript, at 162:17-163:7, 166:1-13; Griscom Testimony, Oct. 23 Transcript, at 54:25-55:4; Walsh Testimony, Oct. 23 Transcript, at 116:1-117:1; P. Exh. 6, at 0025; P. Exh. 106, at 0005, 0015; Peckham Testimony, Oct. 31 Transcript, at 24:16-23 (Urban Dictionary has 330,000 visitors per day).

327. Credit cards are not commonly used for online transactions in Europe and Asia. The effect of COPA would be to divide the Web into two sections, one involving U.S. speakers who largely speak only to U.S. residents and another Web, composed of overseas sites who can speak to anyone including U.S. residents. P. Exh. 25, at 0024.

4. Defendant's Payment Card Expert is not Qualified to Opine in Numerous Areas of His Testimony.

328. Before being retained by Defendant, Mr. Clark had no professional experience with the use of credit cards, debit cards or prepaid cards by minors on the Internet. Clark Testimony, Nov. 14 Transcript, at 177:14-25.

329. Mr. Clark has no expertise in parental conduct, including whether or not parents will supervise or monitor the online activities of minors by looking at payment card billing statements. Clark Testimony, Nov. 14 Transcript, at 92:21-93:23, 115:24-116:9.

330. Mr. Clark's opinion that the use by Web sites of screens requiring credit card information, debit card information, or reloadable prepaid card information will prevent minors from accessing harmful materials does not address: (1) content provided by non-commercial Web sites (Clark Testimony, Nov. 14 Transcript, at 179:2-10); (2) content provided by Web sites that only derive revenue from advertising (Clark Testimony, Nov. 14 Transcript, at 229:11-17; 230:20-24);(3) content provided on the Internet but not the World Wide Web, including, for example, Usenet (Clark Testimony, Nov. 14 Transcript, at 179:11-19); (4) content provided by overseas Web sites that do not use payment cards. Clark Testimony, Nov. 14 Transcript, at 230:8-12.

5. The BitPass Product Is Irrelevant.

331. The Bitpass product, and testimony from Mr. Knopper, Bitpass's CEO, is not relevant to this lawsuit. Defendant has admitted that use of the Bitpass product is not an affirmative defense under COPA. Defendant's Representation, Nov. 9 Transcript, at 88:19-89:6

332. The Bitpass product is not available for use by Web sites that sell sexually explicit content. Knopper Testimony, Nov. 9 Transcript, at 117:14-19.

333. The Bitpass product is only used to facilitate online purchases of digital content; it is not used by Web sites that do not sell digital content. Knopper Testimony, Nov. 9 Transcript, at 100:18-22.

334. Bitpass charges Web sites that use its services fees for each transaction. The fee for small Web sites is 15 percent of each transaction. In addition, Bitpass may charge reporting fees and set-up fees. Knopper Testimony, Nov. 9 Transcript, at 123:3-18.

335. There are no age restrictions for opening a Bitpass account. Minors can obtain their own Bitpass account, and purchase content on the Web with that account. Bitpass does not verify the age of consumers, and Web sites are not provided with the identity or age of consumers who purchase content using their Bitpass account. Knopper Testimony, Nov. 9 Transcript, at 107:23-108:4, 110:2-5, 125:9-13.

336. It is not possible to go to a physical location in the United States to open a Bitpass account or fund the account in person with cash. To fund a Bitpass account, a user in the United States must be willing to provide their funding information over the Internet. Knopper Testimony, Nov. 9 Transcript, at 102:24-103:13.

337. Bitpass tells people using its services that it has the right to sell or share their personally identifiable information with a variety of third parties, for a variety of different reasons, including marketing purposes. Knopper Testimony, Nov. 9 Transcript, at 126:14-128:17.

338. Following a discussion with representatives of Defendant, Bitpass changed the wording on a demonstrative exhibit from "adult verification" to "access verification." Bitpass did so because credit cards do not verify age. Knopper Testimony, Nov. 9 Transcript, at 128:2-129:17.

339. Bitpass has not yet developed an "access verification" product. To date, Bitpass has only spent about 20 hours in connection with this potential product. At least 15 of those 20 hours were spent after the Defendant asked Mr. Knopper to testify. No business plan has been developed, no approval has been given to the product and there is no timetable for its release. No pricing has been set for the product, nor has anyone agreed to use it. It is quite possible that such a product may never be developed by Bitpass. Knopper Testimony, Nov. 9 Transcript, at 129:18-131:10.

D. Data Verification Services are Not a Viable Affirmative Defense.

340. A few companies offer non-payment card-based services and/or products that attempt to verify the age or identity of an individual Internet user. These companies are referred to as data verification services ("DVS"). They seek to accomplish in cyberspace what a clerk checking an ID card or driver's license accomplishes in an adult bookstore, only they do not verify the age or identity of an individual; instead, they merely verify the data entered by an Internet user. Russo Testimony, Oct. 25 Transcript, 196:18-197:1; Meiser Testimony, Oct. 31 Transcript, at 127:25-128:15; P. Exh. 25, at 25; P. Exh. 54, at 367. IDology is one such company. Dancu Testimony, Nov. 9 Transcript, at 143:25-144:15, 161:12-25.

341. DVS technologies seek to distinguish adults from children and to grant access privileges only to adults. DVS companies, in other words, seek to accomplish in

cyberspace what a clerk checking an ID card or driver's license accomplishes in an adult bookstore. P. Exh. 54, at 367.

342. DVS companies rely on public records and some privately acquired information in an attempt to verify information. Russo Testimony, Oct. 25 Transcript, 175:24-176:17; P. Exh. 54, at 92.

343. There are no DVS products that accurately verify age. Russo Testimony, Oct. 25 Transcript, at 97:24-98:8, 182:20-183:13; P. Exh. 25; P. Exh. 54, at 376.

1. How DVS Works.

344. Internet users attempting to access content on a Web page that is using a DVS system will be required to provide specified personal information, such as the person's name, last four digits of the social security number, home address, home telephone number, or driver's license number. The DVS company will check this information against a database of records, and then provide a response to the Web page operator who will have the ability to permit or decline access to that user. Russo Testimony, Oct. 25 Transcript, 95:22-96:10, 181:24-182:19; P. Exh. 25, at 26-27; P. Exh. 54, at 92.

345. The minimum information required by a DVS is first name, last name, street address, and zip code. Russo Testimony, Oct. 25 Transcript, 172:24-173:1; Dancu Testimony, Nov. 9 Transcript, at 160:15-22; P. Exh. 76.

346. The possible responses returned by a DVS are: (1) the data verified does not belong to an adult; (2) the data verified belongs to an adult; or (3) the data cannot be verified. Upon receiving these responses, Web page operators will need to determine

whether or not they will grant access to the online content. Russo Testimony, Oct. 25 Transcript, 96:3-96:10, 181:6-12, 181:24-182:19; P. Exh. 25, at 27; P. Exh. 76.

347. The ability of a DVS to verify information increases when more personal information is provided. Thus, the likelihood that a DVS cannot verify information increases when only minimal personal information is provided. Russo Testimony, Oct. 25 Transcript, 173:21-174:4; P. Exh. 25, at 28-29; P. Exh. 76.

348. IDology claims to verify the information that is provided by a Web page visitor by checking the information against records maintained by a third-party data aggregator, interpreting the response it receives from the data aggregator, and then communicating a response to the Web page operator. Dancu Testimony, Nov. 9 Transcript, at 164:10-166:1.

349. IDology refuses to disclose the identity of its data aggregator. Idology also expressly states that it does not warrant the accuracy or completeness of the information supplied by its data aggregator. It is therefore impossible to independently assess the quality of the information upon which IDology relies to verify information. If the information provided by IDdology's unknown data aggregator is not reliable, the verification attempted by IDology will be equally unreliable. Dancu Testimony, Nov. 9 Transcript, at 249:19-250:1, 250:23-24, 251:22-252:3.

2. Use of DVS Imposes a Financial Burden.

350. DVSs charge a minimum of 37 cents for each verification transaction. The cost can rise to 97 cents per transaction, for a more complete verification service. Each and every time an Internet user comes to a Web page that requires its visitors to pass through a DVS screen, the DVS will charge that Web page operator something in

the range of 37 to 97 cents to perform the verification service. Dancu Testimony, Nov. 9 Transcript, at 221:25-222:4; Russo Testimony, Oct. 25 Transcript, 186:2-6, 192:10-19; Meiser Testimony, Oct. 31 Transcript 146:23-147:17; P. Exh. 25, at 26-28.

351. In addition to the per-transaction fees, DVSs also charge an application fee, a set-up fee, and an integration fee. The application/set-up fees cost a minimum of $195, and the integration fee costs $495. Dancu Testimony, Nov. 9 Transcript, at 222:5-18; Russo Testimony, Oct. 25 Transcript, 192:20-193:4, 195:8-14; P. Exh. 25, at 26-27.

352. IDology claims that it is willing to provide discounts to clients based on the volume of transactions processed, but IDology refuses to disclose the amount of any possible discount. It is therefore impossible to factor any such discounts into the cost of IDology services to a high-volume Web page. Dancu Testimony, Nov. 9 Transcript, at 239:10-240:19, 246:7-9.

353. Almost all of IDology's Web Internet clients charge Internet users to access their content or sell products on their sites. Of all its clients, only two provide content to visitors for free and do not sell products through the Web sites using IDology's data verification services. Those two clients are the third largest tobacco company in the world and the Anheuser Busch company. The ability of these large multinational corporations to pay for IDology's services without passing the costs to the Web page visitors is not representative of the ability of other commercial Web page operators that offer free content or who earn revenue solely through advertising, to pay for similar services. A third client, Zoey's Room, a social networking site for girls, charges $20 for joining the Web site, and thus does not offer its content for free. Dancu Testimony, Nov. 9 Transcript, at 189:5-6, 232:1-9, 232:17-22.

354. It is not economically feasible for a Web page operator, especially one that provides free content, to verify the information of every customer that visits the Web page with a DVS. Russo Testimony, Oct. 25 Transcript, 96:25-97:14; P. Exh. 25, at 30, 33. As one example, Plaintiff Urban Dictionary had approximately 40 million visitors between January and October of 2006. Peckham Testimony, Oct. 31 Transcript, at 24:20-23. If Urban Dictionary had been forced to have its users pass through a DVS, such as IDology, Urban Dictionary would have incurred costs from between $14,800,000 to $38,800,000. Dancu Testimony, Nov. 9 Transcript, at 221:25-222:4.

3. DVS has Significant Effectiveness Limitations.

355. DVS databases do not contain foreign records and cannot verify information for individuals residing outside of the United States who are not United States citizens. This limits the audience of Web sites using DVS products exclusively to Americans whose data can be verified, even though there may be millions of people who might otherwise want to access the speech or content on the Web page, and even though it may be very important to a Web site for its material to be communicated to a worldwide audience. Dancu Testimony, Nov. 9 Transcript, at 253:23-254:16; Meiser Testimony, Oct. 31 Transcript, at 142:9-19; Russo Testimony, Oct. 25 Transcript, at 177:22-178:1, 178:2-5, 180:14-181:1; P. Exh. 25, at 32; P. Exh. 79, at 1.

356. No DVS is able to accurately verify the age of everyone living in the United States, or of all United States citizens or adults. As a result, even adults living in the United States who submit valid and legitimate personal information to a DVS in order to access a Web page will often by denied access to the Web page they have a right to access. The result will be that Web sites using DVSs will be prevented from

communicating with millions of adults in the United States who have the constitutional right to view the speech, but cannot do so. Russo Testimony, Oct. 25 Transcript, 178:5-179:12; Dancu Testimony, Nov. 9 Transcript, at 166:25-167:5; Meiser Testimony, Oct. 31 Transcript, 136:1-8; P. Exh. 25, at 31; P. Exh. 76; P. Exh. 79.

357. It is especially difficult for DVSs to verify young adults (between the ages of 17 and 21) or minors, because there is little data available on younger adults, and very little, if any, data available on minors. Because many individuals in the United States who are over 16 years old cannot have their personal data verified, if Web page operators such as Plaintiffs utilize DVSs to comply with COPA, many adults will not be able to access those Web pages. Dancu Testimony, Nov. 9 Transcript, at 257:22-259:20; Meiser Testimony, Oct. 31 Transcript, at 140:1-19, 155:24-156:10; Russo Testimony, Oct. 25 Transcript, 178:16-179:3; P. Exh. 79, at 4.

358. DVSs have difficulty verifying information for recent immigrants, visa holders, or anyone who is not a United States citizen. Dancu Testimony, Nov. 9 Transcript, at 259:21-260:5; Meiser Testimony, Oct. 31 Transcript, 140:1-19; Pl. Exh. 79, at 4; P. Exh. 76.

359. DVSs have difficulty verifying information when there are significant input or typographical errors in the information submitted by the Web page operator or visitor, or in the public records relied upon by the DVS. The ability of DVSs to verify information is only as good as the information that is provided to it. Dancu Testimony, Nov. 9 Transcript, at 255:13-256:9, Meiser Testimony, Oct. 31 Transcript, at 122:17-123:20; Pl. Ex. 79, at 4.

360. DVSs rely on information from many states' Department of Motor Vehicles ("DMVs"). DVSs do not have access to DMV records for every state in the United States. DVSs are less likely to successfully verify the information of persons from states for which it has no DMV records, making it more difficult for persons from those states to access speech that they are constitutionally entitled to view. Dancu Testimony, Nov. 9 Transcript, at 252:7-10; Meiser Testimony, Oct. 31 Transcript, at 134:11- 135:25.

361. DVSs also rely on information from many states' voting records. DVSs do not have access to the voting records for every state in the United States. DVSs are less likely to successfully verify the information of persons from states for which it has no voting records, making it more difficult for persons from those states to access speech that they are constitutionally entitled to view. Dancu Testimony, Nov. 9 Transcript, at 252:11-13; Meiser Testimony, Oct. 31 Transcript, at 134:11- 135:25.

362. Because not every adult has a driver's license or is registered to vote, Web page operators that are required to employ DVSs have a smaller audience than they would otherwise have because the DVSs effectively exclude individuals who would otherwise be entitled to view the speech. P. Exh. 54, at 370.

363. DVSs also rely on information from many states' property records. DVSs do not have access to the property records for every state in the United States. DVSs are less likely to successfully verify the information of persons from states for which it does not have property records, making it more difficult for persons from those states to access speech that they are constitutionally entitled to view. Dancu Testimony, Nov. 9 Transcript, at 252:14-17.

364. DVSs also rely on state vehicle registration records. DVSs do not have access to vehicle registration records for every state in the United States. DVS are less likely to successfully verify the information of persons from states for which they have no vehicle registration records, making it more difficult for persons from those states to access speech that they are constitutionally entitled to view. Dancu Testimony, Nov. 9 Transcript, at 143:25-144:144:15.

365. Not every adult has a driver's license, or is registered to vote, or owns property, and therefore Web page operators that utilize DVSs have a smaller audience than they would otherwise have because DVSs effectively exclude individuals who would otherwise be entitled to view the speech, and to whom the Web page operator is entitled to speak. P. Exh. 54, at 370.

366. DVSs have difficulty verifying the information of persons recently married, divorced, or who otherwise have legally changed their name. Russo Testimony, Oct. 25 Transcript, 179:4-12; P. Exh. 79, at 4.

367. DVSs have difficulty verifying the information of persons who recently moved. Dancu Testimony, Nov. 9 Transcript, at 257:2-14; Russo Testimony, Oct. 25 Transcript, 179:4-12; P. Exh. 79, at 4; P. Exh. 76. Similarly, if the address provided does not match the data records or if the Web page visitor uses an alternate address, the information will not be verified. Dancu Testimony, Nov. 9 Transcript, at 256:10-257:1, Pl. Ex. 79, at 4.

368. Aside from the inherent limitations of DVSs, DVSs face the additional problem that many Internet users will not provide the personal information necessary to pass through a DVS over the Internet. DVSs entail a loss of privacy for the adult Web

page visitor, both perceived and real. When a DVS is used, the reasonable assumption is that the records are being kept – whether or not they are in practice – and the user has a plausible reason to be concerned that his/her name is associated with certain types of material. This fear of loss of privacy will create a chilling effect on the freedom of adults who wish to access lawful, but controversial material. P. Exh. 54, at 372, 376.

369. The result from this feared loss of privacy will be that many Internet users will not be able to access those Web sites using DVSs, and that the Web sites will be stopped from communicating with those individuals, even if they are adults. *See* Deterrence section, *supra,* II. B.

370. Even for those people who are willing to provide their personal information over the Internet in certain circumstances, many individuals who visit Web sites with sexually explicit, possibly adult-oriented material will have privacy concerns about entering their personal information on such a Web site. Russo Testimony, Oct. 26 Transcript, 41:18-42:16; P. Exh. 25, at 32; *See* Deterrence section*, supra.*

371. There is no evidence in the record establishing that any Web page operators in the adult entertainment or pornography industries are currently using IDology as an age verification device. Prior to being contacted to serve as a witness by Defendant, IDology did not have any customers in the Internet pornography industry, and in fact its contract for services prohibited using Idology products for Internet pornography transactions. Dancu Testimony, Nov. 9 Transcript, at 237:19-239:9.

372. For many Web page operators, like Plaintiffs, this loss of privacy concern will cause large volumes of visitors to turn away from pages requiring information verification prior to accessing content. See Deterrence section, *supra.*

373. Because of these significant limitations, any Web page operator using a DVS will have to turn away a large number of legitimate visitors who will not provide the requested personal information and for whom the DVS cannot accurately verify their information. Russo Testimony, Oct. 25 Transcript, 41:18-42:16, 180:14-181:1; P. Exh. 25, at 31-32.

4. DVS Systems can be Circumvented.

374. DVSs cannot determine whether the person entering information into the Web site is the person to whom the information pertains. Nor is there any way for the person to whom the information pertains to know that his or her information has been used because the DVS companies do not notify people when their information has been verified. Because the DVSs rely on basic personal information, such as a person's name and address, they are prone to abuse and can be circumvented with minimal effort by anyone, including minors, desiring to gain access to Web pages relying on DVSs to verify age. Dancu Testimony, Nov. 9 Transcript, at 260:12-261:12; Meiser Testimony, Oct. 31 Transcript, at 127:23-128:15, 138:3-139:21, 143:23-145:3; Russo Testimony, Oct. 25 Transcript, at 97:24-98:8, 182:20-183:18; Pl. Ex. 79, at 5; P. Exh. 25, at 31.

375. The minimum requirements of a DVS – name, address, and zip code – can easily be circumvented by children. Children generally know the first and last name, street address and zip codes of their parents or another adult. Russo Testimony, Oct. 25 Transcript, 97:24-98:8; Dancu Testimony, Nov. 9 Transcript, at 244:11-245:3. Without a physical delivery of goods and an accompanying visual age verification, neither the DVSs nor the Web page operator can know whether an adult or a child provided the information. Attempting to verify age with this information in a consumer-not-present

transaction is therefore unreliable. Russo Testimony, Oct. 25 Transcript, 98:6-8, 183:2-13; Dancu Testimony, Nov. 9 Transcript, at 245:18-246:5; P. Exh. 25, at 31; P. Exh. 54, at 92-93.

E. Digital Certificates Do Not Serve as an Affirmative Defense.

376. Defendant has admitted that there are no digital certificates that can be used to comply with COPA. P. Exh. 163, at 0001-0002.

F. There are No Reasonable Alternatives to the Enumerated Defenses.

377. Defendant has admitted that no other available or feasible options exist that allow Web sites to restrict access to certain material to minors, while continuing to provide it to adults. 47 U.S.C. § 231(c)(1)(C); P. Exh. 163, at 0001-0002.

378. The services offered by Quova are not an age verification product. Alexander Testimony, Nov. 13 Transcript, at 34:11-13.

III. COPA IS NOT NARROWLY TAILORED BECAUSE IT FAILS TO PROTECT MINORS FROM "HARMFUL TO MINORS" CONTENT.

379. COPA is underinclusive because it fails to reach a substantial amount of speech that implicates the government's interest in protecting children from sexually explicit material. COPA does not regulate "harmful to minors" speech that originates overseas, or that is non-commercial, or that is not communicated "by means of the World Wide Web." Even those individuals operating Web sites providing the subset of Internet communication covered by COPA can easily evade COPA, and thereby immunize themselves from prosecution under COPA, by switching to use of FTP, a protocol COPA does not cover. *See infra*.

A. COPA Fails to Reach "Harmful to Minors" Content Originating Overseas.

380. Only 1 to 1.5 percent of all Web sites on the Internet are adult oriented Web sites- a percentage that is become increasingly smaller as the Internet becomes more widely adopted in the United States and globally. Currently, less than half of the adult Web sites are located in the United States. Zook testimony, Oct. 26 Transcript, at 88:22-89:17, 99:9-100:19; P. Exh. 29, at 6-7, 11; P. Exh. 54, at 101.

381. COPA does not cover content originating overseas. Defendant admitted that COPA likely did not reach overseas Web pages. P. Exh. 55 at 3, 4.

382. Even if COPA had been drafted differently to cover overseas Web sites, COPA cannot be enforced against a speaker who is not subject to U.S. law either because he or she is outside the jurisdiction or for any other reason. P. Exh. 6, at 0037; P. Exh. 54, at 0141.

383. The National Research Council report, commissioned by Congress, concluded that because a substantial percentage of sexually explicit Web sites exist outside the United States, even the strict enforcement of COPA will likely have only a marginal effect on the availability of such material on the Internet in the United States. P. Exh. 54, at 235.

384. The National Research Council report specifically noted that some estimates place as much as 75 percent of adult membership Web sites overseas. P. Exh. 54, at 101.

385. Professor Matthew Zook conducted a study that confirms that there is a substantial amount of sexually explicit content originating overseas. Professor Zook is an expert in Internet Geography who was retained by Plaintiffs to study the geographic

distribution of the owners of Internet adult Web sites. Internet Geography is the study of the geographic location of people producing, creating and managing Web pages, as well as the people surfing the Internet. Zook Testimony, Oct. 26 Transcript, at 53:12-23, 54:2-56:3, 57:1-59:21, 60:14-61:15, 62:6-65:3, 66:22-67:5; 70:22-71:19; P. Exh. 28; P. Exh. 29, at 3.

386. Professor Zook conducted independent research for this engagement, using sound methodology that was the basis of a prior academic research project that was published in a peer-reviewed journal in 2003. Zook Testimony, Oct. 26 Transcript, at 65:4-66:21, 72:18-73:21, 74:24-75:21, 79:16-80:2, 81:11-23, 81:44-82:8, 86:17-20, 96:9-97:13; P. Exh. 29 at 4, 7-8, 10-11, Figure 1; P. Exh. 32. The results of Professor Zook's 2006 research were put in his Expert Report, Plaintiffs' Exhibit 29, admitted into evidence. Zook Testimony, Oct. 26 Transcript, at 71:21-72:16; P. Exh. 29.

387. Professor Zook's study and evidence from other sources demonstrates that a conservative estimate places 32 percent of adult membership sites and 58 percent of free adult Web sites outside the United States. Zook Testimony, Oct. 26 Transcript, at 111:2-112:1; Russo Testimony, Oct. 25 Transcript, at 199:14-201:7, 207:6-209:19, 211:15-213:22; P. Exh. 18-19, Figure 2; P. Exh. 25, at 0033-0036; P. Exh. 27, at 0002; P. Exh. 54, 101; P. Exh. 119, at 0001-0012, 0016-0017.

388. A Web site host location is the location of the computer through which the Web site is placed on the Internet. The host location is unrelated to- and can be completely separated from – the geographic location of a Web site owner, and therefore is not relevant to the question of the geographic distribution of the ownership of Web sites. Zook testimony, Oct. 28 Transcript, at 78:3-79:12, 167:4-14.

389. Defendant's Mewett/Stark study, although it focuses on Web site host location rather than the geographic location of the web page operator, confirms Professor Zook's results. The Mewett/Stark study concludes that approximately 50% of all Web pages categorized by Mr. Mewett as sexually explicit were hosted overseas. More specifically, 55.8% of the Web pages derived from the Google index were hosted overseas and 44.4% of the Web pages derived from the MSN index were hosted overseas. D. Exh. 62, ¶10.

390. The numbers and percentages in the Defendant's Mewett/Stark study that report on "free foreign" Web pages cannot be relied upon because they comprise a very small sample. D. Exh. 83, ¶38; D. Exh. 79, 63; P. Exh. 169; Mewett Testimony, Nov. 8 Transcript, at 31:16-34:24; Stark Testimony, Nov. 8 Transcript, at 170:13-171:5.

391. The numbers and percentages in the Defendant's Mewett/Stark study that report on "free foreign" Web pages cannot be relied upon because by rejecting the Mewett/Stark initial definition of "domestic" and by using a definition of "domestic" that included any Web site that either accepted any international credit card or was linked by as many as five links to a site that accepted any international credit card, they utilized an invalid definition of "domestic." D. Exh. 63, ¶26; Mewett Testimony, Nov. 8 Transcript, at 35:13-38:4.

392. There is undisputed evidence that the high percentage of adult Web sites registered overseas is increasing, and the last five years have seen a corresponding decrease in the percentage of adult Web sites located in the United States. Zook Testimony, Oct. 26 Transcript, at 107:24-108:16, 109:3-16, 112:2-9; P. Exh. 29, at 13-17, Tables 4, 6, 8. Free adult Web sites are migrating at the highest rates. From 2001 to

2006, the United States' share of free adult Web sites dropped from 60 percent to 42 percent. Zook Testimony, Oct. 26 Transcript, at 109:25-111:1; P. Exh. 17-18, Table 9.

393. Increasing numbers of Internet users and producers are located outside of the United States. From 1997 to 2005, the percent of Internet users located in the United States dropped from 75 percent to just 25 percent. Similarly, the number of Top 100 Web sites located in the United States decreased from 94 percent in 1997 to 86 percent in 2000. Of particular relevance is the fact that the percentage of adult Web sites located outside the United States is increasing; 79 percent were located in the United States in 1997, as compared to only 58 percent in 2000. Zook Testimony, Oct. 26 Transcript, at 90:9-91:6, 103:5-104:1; P. Exh. 29, at 12, 20-21, Figure 3, Table 3.

1. There is No Basis for Assuming That Payment Card Companies will Enforce COPA.

394. There is no reason for Web sites that do not sell anything – i.e., sites on which there is nothing for the user to purchase – to have relationships with any of the payment card associations. Those Plaintiffs and other Web speakers who do not sell any objects for purchase directly on their Web sites do not have relationships with any of the payment card companies. Mann Testimony, Nov. 6 Transcript, at 156:6-156:14; Tepper Testimony, Oct. 30 Transcript, at 235:5-8; Lewis Testimony, Oct. 31 Transcript, at 111:11 –112:13; DeGenevieve testimony, Nov. 1 Transcript, at 62:25-63:12; P. Exh. 34.

395. Payment card associations have no mechanisms and no ability to enforce COPA against Web sites that do not have relationships with them. Mann Testimony, Nov. 6 Transcript, at 156:6-14; Russo Testimony, Oct. 25 Transcript, at 83:10-21; Clark Testimony, Nov. 14 Transcript, at 229:11-17; P. Exh. 34, at 0010.

396. Based on the payment card associations' past behavior and present policies, it is highly unlikely that they would enforce COPA against domestic online content providers. The rare situations in which payment card associations have previously enforced laws against online merchants involved inherently illegal transactions and/or laws placing specific obligations on the payment card associations themselves. These situations are not comparable to the enforcement of COPA. Mann Testimony, Nov. 6 Transcript, at 154:9-155:12; 156:6-157:8, 157:9-158:9; Clark Testimony, Nov. 14 Transcript, at 228:6-229:6.

397. Mr. Clark is only familiar with the enforcement of payment card association policies that involve inappropriate use of payment cards. It is the opinion of Mr. Clark that there is not an inappropriate use of payment cards when a Web site gives unrestricted access to harmful to minors content without requiring use of a payment card. Clark Testimony, Nov. 14 Transcript, at 235:8-16, 236:12-23.

398. Based on the payment card associations' past behavior and present policies, it is also highly unlikely that they would enforce COPA against overseas online content providers. Mann Testimony, Nov. 6 Transcript, at 154:9-155:12; 156:6-157:8; Clark Testimony, Nov. 14 Transcript, at 228:6-229:6.

399. That is important because Defendant has admitted that if COPA were to become law, "children would still be able to obtain ready access to pornography from a myriad of overseas web sites." P. Exh. 55, at 0002.

400. For much the same reason, the COPA Commission, the U.S. Department of Commerce, and the Federal Trade Commission have all stated that "Bilateral agreements with foreign governments have emphasized the importance of filtering

technologies rather than the use of government censorship to protect minors from accessing inappropriate material on the Internet." P. Exh. 6, at 0054.

401. It is not Mr. Clark's opinion that payment card associations will enforce COPA against Web sites that are located overseas. Mr. Clark merely testified that payment card associations have the ability to do so. Clark Testimony, Nov. 14 Transcript, at 224:3-20.

402. Despite ample opportunity during depositions and informal discussions, neither Defendant nor Mr. Clark asked the payment card associations whether they would enforce COPA against Web sites that are located overseas. Clark Testimony, Nov. 14 Transcript, at 225:14-228:18.

403. Payment card associations enforce their policies through "Acquiring Banks" or "Acquirers." Acquirers provide bank accounts to merchants, including Web sites, that accept payment cards. Cadwell Testimony, Oct. 31 Transcript, at 161:15-161:21; Bergman Testimony, Nov. 7 Transcript, at 31:23- 32:7; Clark Testimony, Nov. 14 Transcript, at 230:25-231:5; P. Exh. 141, at 0001.

404. Visa requires that Acquirers and merchants, including Web sites, be located in the same Visa region. For example, only Acquirers in the Visa EU region may provide merchant accounts to Web sites located in France. Cadwell Testimony, Oct. 31 Transcript, at 160:17-162:27; Clark Testimony, Nov. 14 Transcript, at 230:25 231:14.

405. There is no indication that non-U.S. Acquirers will enforce COPA against their merchants. Clark Testimony, Nov. 14 Transcript, at 232:25-236:23.

406. There is no indication that non-U.S. Acquirers will be able to determine whether content violates the applicable "community standards" referred to by COPA. Mr. Clark does not know whether French Web sites or European banks will be able to determine whether certain content meets the COPA definition of "harmful to minors." Clark Testimony, Nov. 14 Transcript, at 232:25- 233:10.

B. COPA Fails to Reach "Harmful to Minors" Content That is Non-Commercial.

407. COPA does not reach non-commercial speech. J. Exh. 1, ¶119.

408. Sexually explicit material is available from many non-commercial Internet sources. Focusing primarily on access to sexually explicit material provided by commercial Web sites is likely to have limited relevance to exposure from non-commercial sources. P. Exh. 54, at 387.

C. COPA Fails to Reach "Harmful to Minors" Content That is Not "by means of the World Wide Web."

409. COPA fails to regulate most Internet communication. Browsing the Web is one way in which individuals can use the Internet. The Internet can be used to engage in activities such as sending and receiving emails, trading files, exchanging instant messages, chatting online, streaming audio and video, and making voice calls. J. Exh. 1, ¶ 94.

410. COPA applies to some Web pages in their entirety and others in part. It fails to proscribe "harmful to minors" content communicated by such popular Internet communication methods as email, instant messaging and chat, peer-to-peer, Voice over Internet Protocol, and streaming audio and video. Felten Testimony, Oct. 25 Transcript, passim.

411. COPA's definition of "by means of the World Wide Web" determines what forms of communication it regulates. 47 U.S.C. § 231(a)(1).

412. COPA states that: "The term 'by means of the World Wide Web' means by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol." 47 U.S.C. § 231(e)(1).

413. COPA's technical definition breaks down into roughly three parts. The first part is "placement of material in a computer server-based file archive." A file archive is a system for storing files, but does not include ephemeral storage. The term computer server-based indicates that the file archive must play the role of a computer server. A computer server is a system whose job it is to respond to requests from other computers or programs. Felten Testimony, Oct. 24 Transcript, at 192:19-193:02, 193:17-21, 194:21-23.

414. A standard example of a computer server-based file archive is one that provides Web pages. For instance, there is a computer that stores copies of all of the Web pages that an Internet user can view by going to http://www.uscourts.gov. The pages are stored in an archive. The computer that stores copies of the Web pages is a server. Other computers that make the requests are called clients. Felten Testimony, Oct. 24 Transcript, at 194:24-195:14.

415. The second part of COPA's technical definition is "so that it is publicly accessible, over the Internet." "Internet" is a well-known technical term that refers to a worldwide network of computers. "Publicly accessible" means that anyone can access

the material over the Internet. Felten Testimony, Oct. 24 Transcript, at 195:25-196:09; J. Exh. 1 ¶ 78.

416. Some Web pages are publicly accessible over the Internet because they can be downloaded by anybody anywhere. Other Web pages, many part of what is known as the "deep Web," are not publicly accessible. Email is not publicly accessible over the Internet, because the message is accessible only by the sender and to the recipients. Felten Testimony, Oct. 24, Transcript, at 196:10-19; 199:23-200:08.

417. The third part of COPA's technical definition is "using hypertext transfer protocol or any successor protocol." 47 U.S.C. § 231(e)(1).

418. A protocol is a formalized set of rules that is written down in the language of computer science and that governs an interaction between different computers, usually across a network. A variety of protocols are used on the Internet. Felten Testimony, Oct. 24, at 200:09-17; 202:3-17.

419. Hypertext transfer protocol ("HTTP") is a particular protocol. HTTP is a protocol that allows one computer or program, the "client," to access a file or other content from another computer, the "server." HTTP is often used to download Web pages. It is not the only protocol that can be used to download Web pages. J. Exh. 1, ¶ 111; Felten Testimony, Oct. 24, at 203:02-204:02.

420. A protocol is a "successor protocol" if it (1) was designed after HTTP, (2) was designed to do the same job or fulfill the same essential purpose as HTTP, and (3) uses a design based on that of HTTP. If all three criteria are met, then a protocol is a successor protocol to HTTP. Felten Testimony, Oct. 24, at 204:03-22.

1. COPA Does Not Cover Email.

421. Speech that is communicated over email is not covered by COPA and cannot be prosecuted under COPA. Email is not by means of the World Wide Web. Email messages are not publicly accessible over the Internet. Emails are not generally accessible using HTTP or a successor protocol. Felten Testimony, Oct. 24, at 207:25-208:13.

422. A large amount of communication is conveyed through email. Email is the second most popular use of the Internet among students. Felten Testimony, Oct. 24, at 209:17-20; Def. Exh. 81 at 40.

423. Sexually explicit content is communicated through email, either directly embedded in the email or as attachments. Murphy Testimony, Nov. 1, at 236:15-237:10.

424. It is important that COPA does not cover email because studies indicate that children feel more unsafe due to email than from surfing on the Web. Cranor Testimony, Oct. 24 Transcript, at 133:10-19; P. Exh. 85, at 14.

2. COPA Does Not Cover Instant Messaging and Chat.

425. Instant messaging and chat are communication technologies that allow users to type messages to each other and have those messages displayed immediately. These programs often also allow users to have voice or video conversations in addition to text conversations, and to exchange any type of file that can be stored on a computer. Felten Testimony, Oct. 24, at 211:01-08, 215:18-216:23, 217:02-11. P. Exh. 119.

426. There are a variety of instant messaging programs available for free online. They are easy to download, install and use. Felten Testimony, Oct. 24, at 212:04-22, 217:02-04. P. Exh. 119.

427. Speech that is communicated over instant messaging and chat is not covered by COPA and cannot be prosecuted under COPA. Information communicated through instant messaging and chat is not publicly accessible across the Internet. Also, depending on the instant messaging and chat system being used, a user may or may not be using HTTP. Without conducting considerable technical research, a user would be unable to tell whether he or she is communicating using HTTP. Felten Testimony, Oct. 24, at 217:12-218:11.

428. A great deal of communication takes place through instant messaging and chat. Felten Testimony, Oct. 24, at 218:12-219:22.

429. Sexually explicit content is communicated through instant messaging and chat. Murphy Testimony, Nov. 1, at 236:15-237:10.

3. COPA Does Not Cover Newsgroups.

430. COPA does not apply to newsgroups. J. Exh. 1 ¶ 119. It is easy for minors to install a newsgroup reader and come into contact with adult content on newsgroups. Russo Testimony, Oct. 25 Transcript, at 210:5-12.

4. COPA Does Not Cover Peer-to-Peer.

431. P2P refers to technologies for transferring files between different users. The term P2P refers to a certain technical aspect of the design, specifically that the files are transferred directly from one end user's computer to another end user's computer without the use of an intervening server. Felten Testimony, Oct. 24, at 219:23-220:17. P. Exh. 119.

432. There are numerous P2P programs available for free online. They are easy to download, install and use. Felten Testimony, Oct. 24, at 220:18-20, 221:03-17, 226:11-23. P. Exh. 119.

433. Speech that is communicated over peer-to-peer ("P2P") is not covered by COPA and cannot be prosecuted under COPA. Communication through P2P does not involve use of a computer server-based file archive. Also, some P2P systems do not use HTTP or a successor protocol. A typical user will be unable to tell whether a particular P2P program uses HTTP. Felten Testimony, Oct. 24, at 226:24-227:16.

434. A large amount of speech takes place through P2P. In 1998, P2P technology was quite new and not well-known. Since that time, use of P2P has skyrocketed, and is now very widely used. There are at least 134 peer to peer file sharing programs available to the public to download, almost all of which are free. Felten Testimony, Oct. 24 Transcript, at 228:04-229:22; P Exh. 27 at 0024; P. Exh. 54, at 98.

435. Sexually explicit content is communicated through P2P, and it is increasingly prevalent. In fact, it is much easier to find adult content on peer-to-peer file distribution networks than it is to find adult content on the World Wide Web. In addition to allowing pornography to be accessed by a known word search, some peer to peer programs provide chat rooms that enable users to directly share entire folders of files with one another, including pornographic files. Russo Testimony, Oct. 25 Transcript, at 203:13-204:7, 205:10-19; Murphy Testimony, Nov. 1, at 236:15-237:10; P. Exh. 27 at 0026, 28.

5. COPA does not cover Voice over Internet Protocol.

436. Voice Over Internet Protocol ("VoIP") refers to technologies that enable Internet users to have voice conversations over the Internet. VoIP programs can be used to make voice calls both to other VoIP users and users of traditional telephones. They also enable users to have text chats with other users, the same as traditional instant messaging programs. VoIP programs also support video calls. It is also possible to transfer all varieties of file through VoIP programs. Felten Testimony, Oct. 24 Transcript, at 229:23-230:03, 231:22-234:17. P. Exh. 119.

437. VoIP programs are available for free online. They are easy to download, install and use. Felten Testimony, Oct. 24 Transcript, at 230:14-231:08. P. Exh. 119.

438. Speech that is communicated through VoIP is not covered by COPA and cannot be prosecuted under COPA. VoIP communications are not publicly accessible. VoIP communications are generally not through HTTP or a successor protocol. Also, they do not involve placement of material in a computer server-based file archive. Felten Testimony, Oct. 24 Transcript, at 234:18-235:07.

439. A great deal of communication takes place through VoIP. Skype, a popular VoIP program, claims that tens of millions or perhaps hundreds of millions of people have downloaded their application. Felten Testimony, Oct. 24 Transcript, at 235:08-14.

6. COPA does not cover streaming video and audio.

440. Streaming video and audio is a set of technologies that let users listen to audio streams, similar to listening to the radio, or watch video streams, similar to watching television. Felten Testimony, Oct. 24 Transcript, at 236:15-22. P. Exh. 119.

441. A variety of streaming programs are available for free download on the Internet. Felten Testimony, Oct. 24 Transcript, at 236:14-20, 239:11-17.

442. Speech that is communicated through streaming video or audio is not covered by COPA and cannot be prosecuted under COPA. The protocols streaming programs use are not HTTP or successor protocols. Felten Testimony, Oct. 24 Transcript, at 239:18-25.

443. There are a variety of ways to locate streaming video and audio. One way is to use a Web browser. Another way is to use a program specifically designed for streaming, such as RealPlayer, and type into it the location of the content sought. Some streaming programs give users a set of menus they can navigate through to locate different content. Felten Testimony, Oct. 24 Transcript, at 240:01-22. P. Exh. 119.

444. Streaming video and audio can be displayed by programs specifically designed for streaming, such as RealPlayer. It can also be displayed with a browser window wrapped around it but, in that case, it is still being displayed by Real Player, by a separate program. Felten Testimony, Oct. 24 Transcript, at 240:23-241:04 P. Exh. 119.

445. Even when streaming material is displayed within a Web browser, it is not by means of the World Wide Web. That is because it is not accessible via http or a successor protocol. It is using another protocol, which is designed for streaming, rather than http or a successor protocol. Felten Testimony, Oct. 24 Transcript, at 241:05-15.

446. A large quantity of communication occurs through streaming. Many radio stations broadcast their programming through streaming. Some major TV networks make their shows available via streaming. Also, there are specialized Web sites such as

YouTube that allow individuals to upload files and make them available via streaming. Felten Testimony, Oct. 24 Transcript, at 241:16-242:05.

447. There is a large quantity of sexually explicit content available through streaming. This content is available to minors. Russo Testimony, Oct. 25 Transcript, at 210:14-215:04.

448. Internet content filters are the only technological method of stopping minors from using Internet communications tools such as email, instant messaging and chat, P2P, VoIP, and streaming audio and video. Felten Testimony, Oct. 24 Transcript, at 242:09-14

D. COPA is Easily Evaded Through Conversion to FTP.

449. Even those individuals operating Web sites that are currently covered by COPA could easily evade COPA, and thereby immunize themselves from criminal prosecution under COPA, by using FTP instead of HTTP. Felten Testimony, Oct. 25 Transcript, at 6:02-7:05. P. Exh. 19, 119.

450. FTP stands for File Transfer Protocol. It is a protocol that is often used for downloading information on the Internet. Felten Testimony, Oct. 25 Transcript, at 5:16-18; J. Exh. 1, ¶ 110.

451. FTP is not a successor to HTTP because it meets none of the three requirements for being a successor protocol. FTP was created about two decades before HTTP. Felten Testimony, Oct. 25 Transcript, at 5:19-5:01.

452. It is not difficult for a Web site operator to deliver part or all or a Web site's content through FTP instead of HTTP. Felten Testimony, Oct. 25 Transcript, at 6:02-7:05. P. Exh. 19, 119.

453. For example, a Web site operator can convert individual images delivered using HTTP so that they are delivered using FTP. A Web site operator could convert one page of a Web site so that it is delivered by FTP instead of HTTP. Alternately, a Web site operator could deliver an entire Web site using FTP instead of HTTP. Felten Testimony, Oct. 25 Transcript, at 16:25-17:14. P. Exh. 19, 119.

454. Sexually explicit images can be delivered by FTP instead of by HTTP. It is possible, using FTP, for a home computer user to send a file full of pornographic images to another user on the Internet. Felten Testimony, Oct. 25 Transcript, at 17:15-22, 65:09-16.

455. It takes only a few minutes to convert an image so that it is delivered by HTTP instead of by FTP. Felten Testimony, Oct. 25 Transcript, at 40:10-16.

456. Firewalls do not hinder the conversion of Web sites from HTTP to FTP. Firewalls only filter out FTP content if they have been instructed to do so. There is no reason why CGI scripts cannot be used with FTP just as easily as with HTTP, and using FTP does not create additional security risks. FTP can provide the same functionality that cookies provide. Felten Testimony, Oct. 25 Transcript, at 17:23-19:14, 55:03-12, 56:19-57:05.

457. There is no technical barrier to search engines indexing and delivering FTP pages. Felten Testimony, Oct. 25 Transcript, at 56:02-07.

IV. DEFENDANT FAILED TO PROVE THAT COPA IS THE LEAST RESTRICTIVE ALTERNATIVE.

458. Plaintiffs' expert witness on the alternatives to COPA, Dr. Lorrie Faith Cranor, is an associate research professor in the School of Computer Science at Carnegie

Mellon University. Dr. Cranor also has appointments at Carnegie Mellon in the Department of Engineering and Public Policy, in the Institute for Software Research and in the Human Computer Interaction Institute. Cranor Testimony, Oct. 23 Transcript, at 202:2-15.

459. Dr. Cranor first began studying and evaluating Internet filtering products and other non-filtering Internet control tools for parents to use to control their children's access to the Internet in 1996 in connection with her work at AT&T Labs. Dr. Cranor became the in-house expert for AT&T on matters related to filtering software, consulting with AT&T's business units who were considering offering various different filtering products to their customers, and assisting AT&T's public policy arm in Washington, D.C. in connection with matters related to filtering products. Cranor Testimony, Oct. 23 Transcript, at 215:25-216:25.

460. In connection with her work at AT&T, Dr. Cranor conducted an extensive research study on Internet filtering products and the other Internet parental control tools, such as monitoring children's use of the Internet, and published an authoritative catalog summarizing that research and detailing the various technology and non-technology tools that parents can use to control their children's Internet access. This catalog was based on Dr. Cranor's evaluation of the various filtering products and on informational surveys that were filled out by filtering product companies about their products and by child advocacy groups and consumer groups about their needs and concerns with respect to Internet parental control tools. Dr. Cranor published this catalog in 1998 in connection with the Internet Online Summit, a conference organized by the Internet industry to address the issue of protecting children online. Dr. Cranor was chosen to

present the overview on the existing technology at the Summit. Cranor Testimony, Oct. 23 Transcript, at 217:1-220:15.

461. Dr. Cranor updated her catalog about a year later. Since that time, Dr. Cranor has maintained her research interest in filtering products and non-filtering parental control tools, reviewing most of the different studies that have subsequently been published on filtering products and periodically installing and testing many of the filtering products to see how they work. Cranor Testimony, Oct. 23 Transcript, at 220:16-221:7.

462. Dr. Cranor subsequently testified about Internet filtering products to the COPA Commission, the commission established by Congress as part of the COPA legislation at issue in this lawsuit to evaluate the various technological and non-technological solutions to protecting children on the Internet. Dr. Cranor was chosen to be the first witness to the COPA Commission, to provide an overview of the various technology and parental empowerment tools for parents to use to protect their children on the Internet. Cranor Testimony, Oct. 23 Transcript, at 221:8-222:15.

463. Dr. Cranor has previously served as an expert witness on issues related to communications on the Internet generally, and Internet filtering products and other non-filtering Internet parental control tools specifically, in five previous federal lawsuits. Those cases are: Cyberspace v. Engler, 55 F. Supp. 29 737 (ED Mich. 1999) aff'd 238 F 3d 420 (6th Cir. 2000); PSINet v. Chapman, 167 F. Supp. 2d 878 (WD Va. 2001) aff'd 362 F 3d 227 (4th Cir. 2004); American Booksellers v. Dean, 202 F. Supp. 2d 300 (D. Vt. 2002) aff'd in pert. part 342 F 3d 96 (2nd Cir. 2003); Bookfriends v. Taft, 223 F. Supp. 201 932 (SD Ohio 2002); Southeast Booksellers v. McMasters, 282 F. Supp. 2d

1180 (D. S.C. 2003). Those cases all involved challenges to state versions of COPA. Cranor Testimony, Oct. 23 Transcript, at 222:21-227:5; P. Exh. 1, at 5; P. Exh. 2, at 1-2.

464. In each of those five cases, Dr. Cranor prepared an expert opinion on whether filtering products and other parental control tools were effective alternatives to each state's decision to criminalize "harmful to minors" speech on the Internet. She reached those opinions based on her prior years of research, her review of applicable studies on filtering products, and her own use of many of the filtering products on the market. Her opinion in each of those cases was that there were effective alternatives to the state legislation, including filtering products and other parental empowerment tools. Cranor Testimony, Oct. 23 Transcript, at 222:21-227:5.

465. The legislation at issue in each of these cases was declared unconstitutional in violation of the First Amendment by each federal district court. *See* supra.

466. Dr. Cranor was received by the Court as an expert in Internet filtering devices and the use of the computer and the Internet generally. Oct. 23 Transcript, 227:6-21.

A. Defendant Failed to Prove that Internet Content Filters are Less Effective than COPA.

1. Summary of Internet Content Filters.

467. Internet service providers ("ISPs") and private software companies provide parents with a wide range of technological tools to use to prevent their children from accessing material online that they do not want their children to view. Parents can tailor these tools to their own values and to the age and maturity of their children. These products can be used to block speech that is published overseas, published on non-

commercial sites, or available on the Internet in non-Web-based mediums, such as email, instant messaging, chat, newsgroups, peer-to-peer file sharing, and any other formats other than http. Cranor Testimony, at passim; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 201:18-212:24, 212:25-213:24, 216:12-23, 220:5-221:14; Allan Testimony, Nov. 2 Transcript, at 240:18-241:8; Murphy Testimony, Nov. 1 Transcript, at 210:7-213:25, 217:21-221:7; P. Exh. 6; P. Exh. 11; P. Exh. 54; P. Exh. 86.

468. One of these technological tools is Internet content filtering software, also known as user-based blocking programs. Parents can use Internet content filters to restrict access to certain types of content on the Internet, including sexually explicit content. Filtering products allow parents, among other things, to block access to sexually explicit Web pages, to prevent children from giving personal information to strangers by e-mail or in chat rooms, and to keep a log recording their children's online activity. Cranor Testimony, Oct. 23 Transcript, at 232:11-233:1; Whittle Testimony, Oct. 31 Transcript, at 210:19-212:13.

469. Internet content filters are used frequently by parents, schools and libraries to restrict the Internet access of children, and by employers to restrict the Internet access of their employees. Cranor Testimony, Oct. 23 Transcript, at 232:11-233:1; Kirk Testimony, Nov. 1 Transcript, at 87:16-88:14; Taylor Testimony, Nov. 1 Transcript, at 172:10-18; Smathers Testimony, Nov. 2 Transcript, at 19:14-20:6; Murphy Testimony, Nov. 11 Transcript, at 194:6-196:6.

470. Internet content filters can be programmed or configured in a variety of different ways. They can be set up to restrict materials based on, among other things, the type of content they contain (adult material, information about drugs, hate speech, etc.),

the presence of particular words, the address of the Web site, or the Internet protocol or application used (World Wide Web, email, instant message, peer-to-peer, etc.). Some filters can also restrict access based on time of day, day of week, how long the computer has been connected to the Internet, or which user is logged onto a computer. Allan Testimony, Nov. 2 Transcript, at 204:22-207:16, 236:22-237:7, 238:16-20, 246:19-247:21; Allan Testimony, Nov. 6 Transcript, at 5:22-6:2; Whittle Testimony, Oct 31 Transcript, at 200:2-16, 202:10-203:8, 206:23-212:13, 213:2-15; Murphy Testimony, Nov. 1 Transcript, at 218:23-220:2; P. Exh. 86.

471. Some filtering programs offer only a small number of settings, while others are highly customizable, allowing a parent to make detailed decisions about what to allow and what to block. Filtering products do this by, among other things, enabling parents to choose which categories of speech they want to be blocked and which age setting they want the product to apply. For example, AOL's filtering product enables parents to choose from four different age settings: general (unrestricted); mature teen; young teen; and kids only. Surfcontrol's product has 13 different categories of speech that can be blocked if a parent so desires. Cranor Testimony, Oct. 23 Transcript, at 233:2-21; P. Exh. 86; Allan Testimony, Nov. 2 Transcript, at 205:16-207:16, 240:18-243:2; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 202:10-203:8, 206:23-212:13, 220:5-25; Murphy Testimony, Nov. 1 Transcript, at 210:7-213:25, 217:25-221:7.

472. Some Internet content filters are built into the services provided by ISPs; a family that subscribes to an ISP that provides filtering services can usually take advantage of these services without installing additional software on their computer.

Filters may also be built into cable modems, wireless access points, and other Internet access devices. Filters will also soon be available as part of Microsoft's new operating system, meaning that all computers that come installed with Microsoft's operating system will have built-in parental control features. Cranor Testimony, Oct. 24 Transcript, at 12:23-13:7, 16:14-17:4; Whittle Testimony, Oct. 31 Transcript, at 236:10-13; Allan Testimony, Nov. 2 Transcript, at 243:5-245:22; Murphy Testimony, Nov. 1 Transcript, at Murphy Dep. Tr. at 69:5-70:18; Felten Testimony, Oct. 25 Transcript, at 37:05-14; Sena Testimony, Nov. 2 Transcript at 33:4-6; P. Exh. 86.

473. Filtering products can be used by parents even if they have more than one child. For example, if a family has four children, many filtering products will enable the parent to set up different accounts for each child, to ensure that each child is able to access only the content that the parents want that particular child to access. Cranor Testimony, Oct. 23 Transcript, at 239:11-22; Cranor Testimony, Oct. 24 Transcript at 36:16-38:11. P. Exh. 86 at 15-22, 33-39.

2. Methodology of Internet Content Filters.

474. Filters enable parents and others to control access to the Internet through a variety of different mechanisms, including black lists, white lists and dynamic filtering. Cranor Testimony, Oct. 23 Transcript, at 234:14-20; J. Exh. 1, ¶ 87-92; Allan Testimony, Nov. 2 Transcript, at 205:16-207:16, 240:18-243:2; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 202:10-203:23-212:13, 220:5-25; Murphy Testimony, Nov. 1 Transcript, at 210:7-213:25; P. Exh. 5, 84, 86.

475. Some filters use "black lists" to filter out content. Black lists are lists of Web site addresses (URLs) or Internet Protocol (IP) addresses that a filtering company has determined point to content that contains the type of materials their filter is designed

to block. Some companies offer black lists that are very extensive, containing millions of Web sites, many of which are published in languages other than English. J. Exh. 1, ¶ 87; Cranor Testimony, Oct. 23 Transcript, at 234:21-235:3; Allan testimony, Nov. 2 Transcript, at 205:16-207:16, 240:18-243:2; Whittle Testimony, Oct. 31 Transcript, 200:2-16, 202:10-203:8, 206:23-212:13, 220:5-25; Murphy Testimony, Nov. 1 Transcript, at 210:7-213:25.

476. Black lists are compiled in a variety of ways. A filtering company may use an automated Web crawler to look for and identify new Web pages that may contain content that should be blocked. They may have human employees search for additional sites. They may also run frequent search engine queries using search terms likely to result in content that should be blocked in order to identify new Web pages containing such content. In addition, some companies review industry lists of popular Web sites, or "most viewed" Web sites, to ensure that their products cover those pages that Internet users are most likely to attempt to access. They may also collect reports of URLs that should or should not be blocked from their users, from their business partners, or from governmental entities. Finally, filtering companies may purchase or otherwise acquire lists of Web pages from other entities, including search engines, to supplement the sites they have independently located. Filtering companies typically use many of these techniques together to create as extensive a black list as possible. Cranor Testimony, Oct. 23 Transcript, at 235:4-236:10; Allan Testimony, Nov. 2 Transcript; at 180:16-188:1; 235:16-236:21; Allan Testimony, Nov. 6 Transcript, at 22:11-23:4; Murphy Testimony, Nov. 1 Transcript, at 189:14-194:5, 196:6, 197:11-21, 198:6-21; Pl. Exh. 136; P. Exh. 2.

477. Filtering companies use search engines to locate Web pages for their black lists because most Internet users, including children, find Internet content today by using a search engine. Mimicking the searches a child is likely to make for certain content – i.e., doing what a typical child would do – enables the filtering companies to identify the sites that children are most likely to see and access. Cranor Testimony, Oct. 23 Transcript, at 236:11-21.

478. Even though the Web is very large, only a small fraction of it is actually viewed frequently. To ensure that those parts that are actually being viewed by users have been located, filtering companies review lists of the most popular Web sites because the pages on those sites are the most likely ones that a child will be able to find and access. Cranor Testimony, Oct. 23 Transcript, at 236:22-237:7.

479. Once the URLs are identified, many filtering companies use an automated system to evaluate the URLs and to decide which should be put on the black list. Others have their human employees check those URLs to confirm that they meet the blocking criteria. Some companies require human review of every site included on their content lists to ensure accuracy. Cranor Testimony, Oct. 23 Transcript, at 235:4-236:10; Allan Testimony, Nov. 2 Transcript, at 186:5-187:10; Allan Testimony, Nov. 6 Transcript, at 22:11-23:4; Murphy Testimony, Nov. 1 Transcript, at 189:14-194:5, 196:6, 197:11-21, 198:6-21; Whittle Testimony, Oct. 31 Transcript, at 203:18-204:14; Pl. Exh. 136.

480. Filtering products that use black lists contain mechanisms for frequently updating these lists and providing those updates to their users. Many of these updates are done automatically, without requiring the user to do anything. Cranor Testimony,

Oct. 23 Transcript, at 237:8-238:7; Allan Testimony, Nov. 6 Transcript, at 22:11-23:4; Murphy Testimony, Nov. 1 Transcript, at 188:14-189:13; Pl. Exh. 131, at 1.

481. "White lists" are lists of Web pages that a filtering company has evaluated and determined should never be blocked. J. Exh.1, ¶ 89, 90; Cranor Testimony, Oct. 23 Transcript, at 238:8-12.

482. Filtering companies compile white lists through a variety of techniques similar to those used to compile black lists. Cranor Testimony, Oct. 23 Transcript, at 238:13-19.

483. Most filtering products enable parents, if they desire, to choose to only permit their children to access content that is on a white list. Cranor Testimony, Oct. 23 Transcript, at 238:20-23.

484. In addition to compiling their own black and white lists, many filtering products give parents or administrators the option of creating customized black or white lists by adding or removing specific Web pages to and from the standard lists. For example, AOL allows parents to specify URLs that they want to be blocked or allowed, regardless of the default settings for a particular age category. Many filters allow these customized lists to be created for multiple users, on a user-by-user basis, enabling a parent who has a child who is 16 years-old and a child who is 6 years-old to create separate customized black lists and white lists for each child. In addition, if parents believe their child is mature enough to see some, but not all, sites of a particular type, they can customize their filter accordingly. J. Exh. 1, ¶ 91; Cranor Testimony, Oct. 23 Transcript, at 238:24-239:22; Allan Testimony, Nov. 2 Transcript, at 205:14-207:16, 240:18- 243:2; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 201:18-212:24,

212:25-213:24, 216:12-23, 220:5-221:14; Murphy Testimony, Nov. 1 Transcript, at 210:7-213:25; P. Exh. 86.

485. Many of the filtering products have divided up their lists into multiple categories; parents can decide if they want to block or allow Web pages within each such category. These categories cover far more than just sexually explicit material, enabling parents to restrict their children's access to whatever kinds of content they choose, not just to sexually explicit materials. For example, in addition to "adult" content, many of the filters have categories such as drugs, weapons, violence, hate speech, and other subjects which some parents might find inappropriate for their children. Some companies that offer multiple content categories allow parents to place a particular site within whichever category they choose, even if this is not the default setting, enabling parents to change decisions made by the filtering company if the parent disagrees with the company's categorization. Cranor Testimony, Oct. 23 Transcript, at 233:22-234:1; Allan Testimony, Nov. 2 Transcript, at 205:14-207:16, 240:18- 243:2; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 201:18-212:24, 212:25-213:24, 216:12-23, 220:5-221:14; Murphy Testimony, Nov. 1 Transcript, at 198:22-201:13, 210:7-213:25; Pl. Exh. 131; P. Exh. 2; P. Exh. 86.

486. In addition to relying on black lists and white lists, many filters also use real-time, dynamic filtering techniques. Instead of basing blocking on previously-made lists, real-time filtering analyzes the content as it is being requested to make a determination as to whether or not it should be blocked. J. Exh. 1, ¶ 92; Cranor Testimony, Oct. 23 Transcript, at 239:23-240:5.

487. Dynamic filtering products analyze content in real-time by evaluating and processing a number of different parts of the content, both what the user can actually see on the Web page, and the various hidden pieces of information contained with the content that are part of its software code or script, known as the "metadata." Among other things, real-time filters analyze the words on the page, the pictures, the metadata, the file names for images, the URLs, the links on a page, the size of images, the formatting of the page, and other statistical pattern recognition features, such as the spatial patterns between certain words and images, which can often help filters categorize content even if the actual words are not recognized. Cranor Testimony, Oct. 23 Transcript, at 240:6-244:18.

488. In addition to analyzing the content of Web pages, dynamic filters also take the context of the page into consideration, to ensure that the determinations are as accurate as possible. For example, many companies will develop templates that provide additional context to teach the software how to recognize certain contexts – for example, to block the word "breast" when used in combination with the word "sexy," but not when used in combination with the words "chicken" or "cancer." The software analyzes context, in part, by utilizing statistical pattern recognition techniques to identify common features of acceptable and unacceptable Web pages, depending on the context in which the content appears. Cranor Testimony, Oct. 23 Transcript, at 243:5-244:6; Allan Testimony, Nov. 2 Transcript, at 223:2-23; 232:3-10; Whittle Testimony, Oct. 31 Transcript, at 201:4-17, 204:17-205:25; Pl. Exh. 136, at 1, 7-10,14-17.

489. Filtering companies use artificial intelligence or machine-learning techniques to teach their software how to determine in real-time whether content should

or should not be blocked if it is not already on a list. This training process typically works by showing the software a large number of pages that should be blocked and a large number that should not be blocked, and then teaching the software how to distinguish between the "good" and "bad" content, telling the software when it makes correct and incorrect decisions, and then re-training it accordingly so the same mistakes are not repeated. This training process is repeated a number of times until the software is highly accurate in distinguishing between the good and bad content. This machine-learning process is highly effective in training the filtering software, and can sometimes obtain levels near agreement with human performance levels. Similar machine-learning techniques are used in a variety of different software applications, such as spam filters, and are relied upon to train software to make real-time determinations. Cranor Testimony, Oct. 23 Transcript, at 240:6-241:14; Allan Testimony, Nov. 2 Transcript, at 198:16-204:9; P. Exh. 54, at 421.

490. Some filters apply these types of real-time techniques to image blocking, just as they do to text blocking. Although image-filtering techniques by themselves tend to be less accurate than text filtering techniques, image filtering can be effective when used in combination with text filtering techniques – for example, examining both images and the textual image captions to determine whether content should be blocked. Indeed, studies done by Rulespace in connection with their mobile filtering product indicate that their image filter is 87 percent accurate if there is no text whatsoever on a page, and when the image filter is combined with their text-based product, the filter is 99.48 percent accurate. Cranor Testimony, Oct. 23 Transcript, at 247:10-18; Allan Testimony,

Nov. 2 Transcript, at 211:17-215:9, 231:3-9; Allan Testimony, Nov. 6 Transcript, at 14:10-17:19; Murphy Testimony, Nov. 1 Transcript, at 207:3-209:15; P. Exh. 2.

491. Filtering products can also block images if the images are located on pages that trigger the ordinary blocking criteria due to, for example, the text on the page, the URL, the links on the page, the metadata, or any of the other features that filters analyze, such as the format and size of the images. Thus, if there is an image on a page and the textual caption for it, or the headline on the page, indicates that the image likely falls into a certain category, the filter will be able to block the image from being accessed by evaluating all of the text on the page. In the same manner, even if there is not a caption for the image, and nothing else on the page indicates that the image is likely to be adult material, if there is anything in the metadata or the other unseen file data that indicates that the image is inappropriate for children, filters will be able to analyze that hidden content and block the image in that manner, if appropriate. That is important because every image needs to have a file name associated with it, even if the user cannot see it. Cranor Testimony, Oct. 23 Transcript, at 247:10-248:25.

492. Metadata is used to allow search engines to locate and recognize sites easily. Web site developers usually include metadata to increase the chances that search engines will include their site near the top of a list of search results. Because filtering companies use search engines to find potentially inappropriate sites, they are likely to find the large majority of sites with inappropriate images that users might actually see. Murphy Testimony, Nov. 1 Transcript, at 190:19-191:15, 209:16-210:5; Cranor Testimony, Oct. 23 Transcript, at 241:15-242:20; P. Exh. 2.

493. Many filtering products utilize the different techniques of white lists, blacklists and dynamic filtering together to increase the effectiveness and accuracy of their products, so that there are several different layers of filtering that content must pass through before it can be accessed by a child. Thus, even if a Web page is not on a white list or blacklist and the filter does not yet know how to treat it, the real-time filtering portion of the product will be able to block it if it should be blocked. Cranor Testimony, Oct. 23 Transcript, at 245:7-246:3; Whittle Testimony, Oct. 31 Transcript, at 201:3-17; Murphy Testimony, Nov. 1 Transcript, at 221:10-222:24.

3. Non-Content Filtering Aspects of Filtering Products.

494. In addition to their content filtering features, filtering products have a number of additional tools to help parents control their children's Internet activities. Other tools available to parents include monitoring and reporting features that allow supervising adults to know which sites a minor has visited and what other types of activities a minor has engaged in online. AOL, for example, offers a feature called AOL Guardian, which provides a parent with a report indicating which Web sites a child visited, which sites were blocked, the number of emails and instant messages a child sent, and to whom a child sent email or instant messages. Surfcontrol similarly provides parents with reports of the sites a child has visited, as well as those that were blocked; their product also has the ability simply to monitor a child's activity without actually blocking anything, if a parent prefers that option. Some of the products, such as Contentwatch's filter, have features that permit parents to monitor their child's Internet activities remotely, for example, while they are at work, and some products even send email alerts to parents when inappropriate material is accessed by a child so that, if a parent so desires, it can supervise their child's Internet activities even when they are not

physically with the child. Cranor Testimony, Oct. 23 Transcript, at 234:2-13, 249:21-251:15; Cranor Testimony, Oct. 24 Transcript, at 28:5-29:13. P. Exh. 2; P. Exh. 86, at 10-13, 32; Whittle Testimony, Oct. 31 Transcript, at 210:2-212:13; Murphy Testimony, Nov. 1 Transcript, at 218:23-220:23.

495. These monitoring and reporting features provide valuable tools to parents. For example, depending on their preferences, if a parent informs their children that their Internet activity is being monitored, the children may well avoid accessing inappropriate material because they know they will not be able to do so undetected. Conversely, if parents decide not to so inform their child, they have the option of seeing if any inappropriate material is accessed, and then discussing that situation with the child to explain why it is or is not appropriate for the child to access that material. Cranor Testimony, Oct. 23 Transcript, at 251:16-25.

496. Several filtering products also provide parents with the option of having a warning appear before a child's access to certain material is permitted, rather than having the material blocked. The child will then have the option of going into the site, if he or she believes it is appropriate to view, or not going into the site, if it is deemed to be inappropriate or undesired. This warning mechanism serves to prevent children from accidentally encountering material they do not wish to see. Cranor Testimony, Oct. 23 Transcript, at 234:2-13, 249:21-250:17.

497. Many filtering programs also offer parents the ability to restrict the times of day that a child can use the Internet, or to control the total amount of time in a given day that a child may use it. Filtering software can similarly restrict Internet access by days of the week, making it possible for parents to make sure that their children only

access the Internet when an adult is home to supervise. Cranor Testimony, Oct. 24 Transcript, at 5:9-6:8; Whittle Testimony, Oct. 31 Transcript, at 210:2-212:13; Murphy Testimony, Nov. 1 Transcript, at 218:23-220:23; P. Exh. 86 at 10.

498. Filtering programs can also be used by parents to prevent their children from having any access to parts of the Internet other than the World Wide Web. Filters can be used to block access to any Internet applications which parents do not want their children to have any access to, such as email, chat, instant messaging, newsgroups, message boards and peer-to-peer file sharing. Cranor Testimony, Oct. 24 Transcript, at 5:18-6:25; Allan Testimony, Nov. 2, at 236:24-237:3, 1; 238:11-20; Allan Testimony, Nov. 6 Transcript, at 5:22-7:8; Whittle Testimony, Oct. 31 Transcript, at 202:10-209:24; 212:25-213:15, 220:14-20; Murphy Testimony, Nov. 1 Transcript, at 217:19-221:7235:21-238:13; P. Exh. 6, 54, 86; J. Exh. 1, ¶ 94.

499. In addition to blocking access to these applications completely, some products provide parents with the option of providing limited access to these Internet applications. For example, instant messaging and email may be permitted, but some of the products will only permit the sending and receiving of messages from certain authorized individuals, and will block e-mails or instant messages containing inappropriate words or any images. Filtering programs can also completely prevent children from entering or using chat rooms, or they can merely filter out any inappropriate words that come up during a chat session. Cranor Testimony, Oct. 24 Transcript, at 7:1-17; Allan Testimony, Nov. 2, at 236:24-237:3, 1; 238:11-20; Allan Testimony, Nov. 6 Transcript, at 5:22-7:8; ; Whittle Testimony, Oct. 31 Transcript, at

202:10-209:24; 212:25-213:15, 220:14-20; Murphy Testimony, Nov. 1 Transcript, at 217:19-221:7235:21-238:13; P. Exh. 6, 54; P. Exh. 86, at 6-7.

500. Many of the products can also be set up to prevent children from inadvertently or intentionally sending out personal information, such as a home address or telephone number, and to block children from receiving downloads, attachments, or file transfers through any means. Cranor Testimony, Oct. 24 Transcript, at 7:18-8:7; Allan Testimony, Nov. 2 Transcript at 236:22-240:17; Allan Testimony, Nov. 6 Transcript at 5:9-8:24; Whittle Testimony, Oct. 31 Transcript at 201:18-209:24, 212:25-213:24, 219:16-221:14; Murphy Testimony, Nov. 1 Transcript, at 217:19-221:7, 235:21-239:15; P. Exh. 54, at 0300, 0304, 0319.

4. Filters are Widely Available.

501. Filters are widely available and easy to obtain. Numerous filtering products are sold directly to consumers, either in stores or over the Internet. Filters are also readily available through ISPs. Because ISPs offer filtering products, a parent does not have to do anything to obtain a filter other than to activate it through the ISP's Web site or to call the ISP. Cranor Testimony, Oct. 24 Transcript, at 8:8-9:9.

502. Most of the ISPs offer filtering products to their customers for free. AOL's filtering product is now even available for free to anyone who wants to use it, even non-AOL subscribers. Cranor Testimony, Oct. 24 Transcript, at 9:10-24.

503. Non-ISP filtering products vary in cost, ranging from approximately $20-$60. Cranor Testimony, Oct. 24 Transcript, at 8:8-17.

504. Most of the filtering products offer money-back guarantees or free trial periods, so that a parent can simply download a filtering product for free over the Internet and then use it for a set time period to see if it is something that they want to

continue using before being required to pay anything or to decide for certain whether it is a product they want to use. Cranor Testimony, Oct. 24 Transcript, at 12:12-22; Eisenach Testimony, Nov. 13 Transcript, at 177:8-25.

505. Filters will also imminently be freely available because they will be pre-installed in all computers using Microsoft's new operating system, Vista. Microsoft has announced plans to launch Vista by January 2007. Vista's content filter will provide features similar to what is found in most current filtering products, including the ability to select which categories of speech should be filtered. Vista's filter will also provide parents with other access control tools, such as time management, the ability to filter non-Web Internet applications like email, and the ability to block or restrict access to online games. Cranor Testimony, Oct. 24 Transcript, at 12:23-13:7, 16:14-17:4; P. Exh. 2.

506. Vista will be compatible with other companies' Internet content filters, meaning that if a parent does not like how Microsoft has classified Web pages, a parent will be able to use another company's classifications simply by configuring them through the standard Vista control panel. Cranor Testimony, Oct. 24 Transcript, at 16:14-17:4.

507. Anyone who has Vista installed on their computer will automatically have free access to these filtering tools. Because the vast majority of personal computers used at home – approximately 90 percent – come pre-loaded with Microsoft's current Windows operating system, the vast majority of computers will soon have built-in, free, compatible filters, meaning that a parent will not have to install or do anything to obtain a filtering product. Cranor Testimony, Oct. 24 Transcript, at 17:5-18:2.

508. Microsoft has also announced that for those computers not using the new operating system, it will soon be making a free content filter available through their Windows Live Web site, which will enable anyone to download and use Microsoft's parental controls software. Cranor Testimony, Oct. 24 Transcript, at 18:3-12.

509. Information comparing the relative quality, price and differing features of the Internet content filtering products is readily available to consumers, for free, through a variety of different sources. Most ISPs have information on their Web sites about the different filtering options that are available for parents. Indeed, a separate statutory provision not challenged here, 47 U.S.C. § 230(d), requires ISPs to notify all new customers that parental control protections such as filters that may limit Internet access to inappropriate material are commercially available. Cranor Testimony, Oct. 24 Transcript, at 9:25-10:12; J. Exh. 1, ¶ 102.

510. Many schools and PTA organizations have also taken it on themselves to provide information about filtering products to parents. Cranor Testimony, Oct. 24 Transcript, at 9:25-10:12.

511. Several major Web sites exist solely to provide these resources to parents. For example, the GetNetWise.org Web site provides users with a plethora of information about the different filtering and non-filtering Internet parental control tools available for parents to use, including a catalog of the different filtering products which provides parents with the names and different features of various filtering products. Cranor Testimony, Oct. 24 Transcript, at 9:25-12:1. P. Exh. 87, at 4-5.

512. Organizations such as Consumer Reports have also published studies and evaluations of the various filtering products that are available online to parents. These

resources provide parents with easy-to-understand recommendations about which filtering products may best fit their individual needs. Cranor Testimony, Oct. 24 Transcript, at 70:9-22.

5. Internet Content Filters are Easy to Use.

513. Filtering programs are easy to install, configure, and use. Cranor Testimony, Oct. 24 Transcript, at 21:3-39:7; P. Exh. 13 at 10-11; P. Exh. 3; P. Exh. 6; P. Exh. 54; P. Exh. 85, at 4; P. Exh. 86.

514. Dr. Cranor is in charge of Carnegie Mellon's Usable Privacy and Security Laboratory. Dr. Cranor directs the lab, which has about a dozen graduate students and some other faculty members. The lab conducts research on usability issues related to a variety of privacy and security-related software. Usability refers to the experience that a user will have with a computer and how easy or hard it is for the user to use the computer to complete the tasks the user is trying to use it for. Cranor Testimony, Oct. 23 Transcript, at 202:22-203:20.

515. The lab has a user testing laboratory where they run studies by bringing in actual human users to use various computer tools. Dr. Cranor and others observe these users and ask them a series of questions to analyze how easy or hard it is for them to use the software being tested. In the past year, Dr Cranor and her lab have conducted about a half dozen of these usability studies. Cranor Testimony, Oct. 23 Transcript, at 202:22-203:20.

516. In addition to these formal laboratory studies, Dr. Cranor is also regularly involved in conducting usability surveys of users, and personally examining software products to determine its likely usability for ordinary computer users. Dr. Cranor has been involved in several dozen formal surveys. Software usability experts like Dr.

Cranor conduct these informal product tests because they can generally determine how usable software is by inspecting and running the software to see how it performs, especially in areas known to pose problems for users. Cranor Testimony, Oct. 23 Transcript, at 204:25:205:14.

517. Dr. Cranor has been evaluating the usability of filtering products and periodically testing the products for the past decade in connection with her work for the Internet Online Summit, her testimony before the COPA Commission, and her expert testimony in the five previous lawsuits challenging state versions of COPA. Her expert opinion in each of those prior instances was that filtering products are easy to install and use. Cranor Testimony, Oct. 24 Transcript, at 18:13-19:1.

518. In connection with her analysis in this case, Dr. Cranor installed and tested several of the filtering products currently on the market. Informal testing like she conducted is one of the standard steps in the usability testing field, and is called a "heuristic evaluation." Because software usability experts like Dr. Cranor know what sorts of issues typical computer users find problematic, by personally testing the software and conducting a heuristic evaluation, an expert can quickly get a high level overview of the overall usability of the product. Cranor Testimony, Oct. 24 Transcript, at 167:19-168:10.

519. Dr. Cranor's heuristic evaluation confirmed her prior research, and what she knew from the existing literature: filtering products are very easy to install and use. In fact, the current versions of the products have improved over time and are even easier to use than the older versions. Cranor Testimony, Oct. 24 Transcript, at 19:2-13, 168:11-18.

520. Dr. Cranor's opinion is consistent with the findings of the various filtering studies that have been conducted over the years, including studies prepared for Defendant. Those studies have all consistently found that many filtering products are very easy for parents to install and use. For example, a study prepared by a company called Etesting Labs for the Defendant, entitled "U.S. Department of Justice Web Content Filtering Software Comparison," concluded that all four of the products tested were "quite easy to install and configure." A study conducted for NetAlert and the Australia Broadcast Authority similarly concluded that certain products, such as AOL's filter, were quite easy to use and install. Cranor Testimony, Oct. 24 Transcript, at 57:9-18, 68:7-21. P. Exh. 3 at 4; P. Exh. 6; P. Exh. 54; P. Exh. 85, at 4.

521. Because there have been a number of studies documenting the usability of filtering software, and because those studies have consistently found – consistent with Dr. Cranor's own research and heuristic evaluations – that filters are easy to install and use, it was not necessary for Dr. Cranor to conduct her own formal study of the usability of filtering software. Cranor Testimony, Oct. 24 Transcript, at 52:5-76:5, 78:3-18.

522. Almost all parents will be able to install filtering products and use them by selecting from one of their standard settings. Many filters, such as AOL Parental Controls and Cybersitter 9.0, have user interfaces that are quite easy to use and that make it easy for users to create customized settings, especially if all they are concerned about blocking is adult material. Cranor Testimony, Oct. 24 Transcript, at 19:19-20:7, 20:19-21:2, 27:1-24; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 206:23-212:13; Murphy Testimony, Nov. 1 Transcript, at 221:8-224:5; P. Exh. 2; P. Exh. 6; P. Exh. 54; P. Exh. 85, at 4; P. Exh. 86, at 8-9.

523. Installing and setting up a filter will usually take a typical computer user about five to ten minutes, but no more than ten or fifteen minutes. The installation and set-up process is not technically complex and does not require any training or computer background. Cranor Testimony, Oct. 24 Transcript, at 21:3-22:8. P. Exh. 86.

524. Configuring a filtering product for more than one child is straightforward and easy with many products. For example, it takes about one minute to set up an account for an additional child using AOL's product. Cranor Testimony, Oct. 24 Transcript, at 36:16-38:11. P. Exh. 33-39.

525. Filtering software is no more difficult to install or use than other software that is widely used every day. Cranor Testimony, Oct. 24 Transcript, at 22:9-18; P. Exh. 2; P. Exh. 13, at 11-12.

526. Although there were occasional user complaints about latency (delay) with early-version filtering products, latency is not an issue with today's filtering products. Existing filters do not usually cause any significant or noticeable delays. The amount of time it typically takes filters to look URLs up in black lists and white lists is generally imperceptible, much less than one second for each request. Cranor Testimony, Oct. 24 Transcript, at 39:24-40:8. Allan Testimony, Nov. 2 Transcript, at 220:1-222:16; Allan Testimony, Nov. 6 Transcript, at 13:4-14:8; Whittle Testimony, Oct. 31 Transcript, at 226:5-23, 6:14-21.

527. Most filtering products do not pose any compatibility issues for computers, meaning that using filters will not affect the typical user's ability to use other computer software. Cranor Testimony, Oct. 24 Transcript, at 40:9-41:6.

528. Installation problems and other technical issues, like compatibility, are disappearing as more and more people use filtering that is bundled with their ISP service or provided on the network rather than on each individual personal computer. As a result of these developments, users no longer need to install stand-alone filtering programs on their personal computers, and bundled filters are by definition compatible with a user's Internet service. Murphy Testimony, Nov. 1 Transcript, at 238:14-239:15; Allan Testimony, Nov. 2 Transcript, at 228:8-230:8, 240:20-241:8; P. Exh. 2.

529. Microsoft's new operating system, Vista, will similarly ease any technical problems, because it will contain filters that, as part of the operating system itself, will work with any other program that is designed to be compatible with it. Cranor Testimony, Oct. 24 Transcript at 41:8-42:6.

6. Filters Cover More Speech than COPA.

530. Filtering products block both Web pages originating from within the United States and Web pages originating from outside the United States. It does not make a difference to filtering products where a page originates from, because the filter is analyzing the content of the page, not the location from which it came. Cranor Testimony, Oct. 24 Transcript at 46:20-47:8. P. Exh. 6, 54; Allan Testimony, Nov. 2 Transcript, at 185:6-12; Whittle Testimony, Oct. 31 Transcript, at 15:2-16:17; Murphy Testimony, Nov. 1 Transcript, at 224:6-14, 226:6-228:21; Pl. Exh. 133.

531. Filtering products block both non-commercial and commercial Web pages. It does not make a difference to filtering products if a page is from a non-commercial or a commercial entity. Cranor Testimony, Oct. 24 Transcript at 47:9-18; P. Exh. 6, 54; Whittle Testimony, Oct. 31 Transcript,. at 202:7-9; Allan Testimony, Nov. 2 Transcript, at 246:6-11.

532. Filtering products block both Web pages that are available for viewing for free and Web pages for which users have to pay to view. Cranor Testimony, Oct. 24 Transcript at 47:19-24.

533. Filtering products can be used by parents to block material that is distributed on the Web and on the other widely used parts of the Internet through protocols other than http. Specifically, filters can be used to block any Internet applications, including email, chat, instant messaging, peer-to-peer file sharing, newsgroups, streaming video and audio, Internet television and voice-over Internet telephone service. J. Exh. 1, ¶ 95; Cranor Testimony, Oct. 24 Transcript at 47:25-48:19; P. Exh. 6, 8, 54, 86, 88; Allan Testimony, Nov. 2 Transcript, at 236:22-239; 246:19-248:10; Allan Testimony, Nov. 6 Transcript, at 5:22-8:23; Whittle Testimony, Oct. 31 Transcript, at 207:17-209:24, 212:25-213:15, 220:14-20; Murphy Testimony, Nov. 1 Transcript, at 203:18-204:3, 217:19-218:22.

534. Filtering products can block new Internet applications that have not yet even been introduced because they can be configured to permit only certain types of Internet traffic to be accessed. Cranor Testimony, Oct. 24 Transcript at 48:8-19.

535. Filtering products will also better protect children on the Internet than COPA because they reach a far broader range of content than COPA, enabling parents to restrict their children's access to whatever kinds of content they choose, not just to harmful to minors materials. For example, many products include categories like Violence, Drugs, Alcohol and Tobacco, Weapons and Criminal Skills, in addition to Nudity/Adult material. Cranor Testimony, Oct. 23 Transcript at 233:22-234:1; P. Exh. 5, 6, 7, 8, 54; Allan Testimony, Nov 2 Transcript, at 204:12-207:13; Whittle Testimony,

Oct. 31 Transcript, at 202:20-203:2; Murphy Testimony, Nov. 1 Transcript, at 198:22-204:3; Pl. Exh. 131.

536. Filtering products also provide a more flexible solution than COPA because filtering products can be tailored to meet the individual values, desires, and needs of Internet users, and the age and maturity of a child. The wide range of user-based filtering options permits parents and families to choose those options which are most consistent with their own family values and the circumstances of their children, including the age and maturity of each child, not the values of some other family or community. Cranor Testimony, Oct. 24 Transcript, at 26:14-27:24, 37:12-20, 73:20-74:8. P. Exh. 86, at 8-9; P. Exh. 5, 6, 7, 8, 54, 84, 85, 86, 88; Allan Testimony, Nov. 2 Transcript, at 205:14-207:16; Whittle Testimony, Oct 31 Transcript, at 200:2-16, 203:3-212:24; Murphy Testimony, Nov. 1 Transcript, at 210:7-213:25, 219:24-221:7.

537. Filtering products offer complete flexibility in that parents can turn them off any time they do not want to block material for themselves, other adults, or for their children. As a result, the potential for overblocking problems is greatly lessened in the context of voluntary parent-initiated filtering. P. Exh. 2; P. Exh. 86; Murphy Testimony, Nov. 1 Transcript, at 220:24-221:7.

7. There Are No Substantive Differences Between Filters Marketed for Use on Home Computers and Enterprise Filters.

538. The filtering products provided by ISPs are business or "enterprise" filtering products. Parents using filters provided by ISPs on their home computers are therefore using enterprise filters, even though they are using them on their home computers. Cranor Testimony, Oct. 24 Transcript at 43:19-44:11.

539. From a technological standpoint, there are not many differences between filters marketed for use in a home and filters marketed to businesses. The differences are not in the core filtering technology, and not in the way filters operate or block content. Instead, the differences are primarily in the way the products can be deployed, because in a business setting, the business will want to install the product on one central computer and then have it run on hundreds of individual computers, without the need to install it on all of those computers. That desire is not present in a home setting, so most products that are marketed for use in a home do not include all of the corporate management tools that enterprise filters contain. Cranor Testimony, Oct. 24 Transcript at 43:19-45:18.

540. Another reason why there are no major differences between enterprise and home filters is that many filtering companies offer both a home and enterprise filtering product. Because of economies of scope and complementarities in production between the two markets, these companies have essentially developed one technology that powers both of their products. Cranor Testimony, Oct. 24 Transcript at 43:19-44:11; Eisenach Testimony, Nov. 13 Transcript, at 184:09-18, 185:15-18.

541. Technology for corporate filtering products can trickle down to home filtering products. Eisenach Testimony, Nov. 13 Transcript, at 185:04-14. To the extent the market for enterprise filtering impacts the market for home ICF, the market for ICF software is broadened. Eisenach Testimony, Nov. 13 Transcript, at 183:16-184:08.

542. Because there are not significant differences in the filtering technologies driving filters marketed for use in the home and in business settings, there are no reasons

why home products would be any more or less effective at blocking inappropriate content than enterprise products. Cranor Testimony, Oct. 24 Transcript at 45:19-46:10.

543. From a technical perspective, there is no reason why a parent who wanted to use a filtering product marketed for use in a business setting could not use that product in their home, as long as they had the right kind of computer and operating system at home. Cranor Testimony, Oct. 24 Transcript at 46:12-19.

8. Filtering Products Provide an Effective Solution for Parents.

a. In General.

544. Filtering products are an effective tool to prevent children from accessing material deemed inappropriate for them. Cranor Testimony, Oct. 23 Transcript, at 76:5; Cranor Testimony, Oct. 24 Transcript, at 49:5-18; Allan Testimony, Nov. 6 Transcript, at 17:20-18:12; Whittle Testimony, Oct. 31 Transcript, at 216:7-12; Murphy Testimony, Nov. 1 Transcript, at 194:6-196:6, 221:8-222:24.

545. Filters work especially well at blocking pornographic material. Although they are not perfect, filtering products block the vast majority of the material on the Web that is sexually explicit and that might be considered harmful to minors. Cranor Testimony, Oct. 24 Transcript, at 49:19-50:1, 55:8-23; Kirk Testimony, Nov. 1 Transcript, at 88:15-24; Taylor Testimony, Nov. 1 Transcript, at 174:22-175:21; Smathers Testimony, Nov. 2 Transcript at 20:7-12; Allan Testimony, Nov. 6 Transcript, at 14:10-18:12; Whittle Testimony, Oct. 31 Transcript, at 216:7-12; P. Exh. 3, at 0001-0005, 0044; P. Exh. 6, at 0019-0022; P. Exh. 11, at 0005-0006; P. Exh. 85, at 0004.

546. Individual filtering products vary in how effective they are at both accurately blocking intended material and not inadvertently blocking appropriate material. The better products are very good at blocking intended material and have very

low rates of erroneously blocking material. Cranor Testimony, Oct. 24 Transcript, at 55:8-23; P. Exh. 3, at 1, 44, 45; P. Exh. 168-170, 260; Allan Testimony, Nov. 6 Transcript, at 17:20-18:12; Whittle Testimony, Oct. 31 Transcript, at 216:7-12; Murphy Testimony, Nov. 1 Transcript, at 194:6-196:6, 221:8-222:24.

547. Filters provide parents with a flexible range of options that parents can choose from. Filters can be made more restrictive or less restrictive and, thus, can block more or less material, depending on the individual desires of parents. The more willing a parent is to have some material inadvertently blocked, the more effective the product will be at blocking virtually all sexually explicit material. If a parent wants to make sure that his or her child does not have access to absolutely any sexually explicit material, the parent can set the filtering product accordingly and, in doing so, can make sure that there is an extremely low chance that such material will be accessible. Cranor Testimony, Oct. 24 Transcript, at 49:5-18; Stark Testimony, Nov. 8 Transcript, at 97:20-98:14 (metal detector discussion); Neale Testimony, Nov. 9 Transcript, 62:6-63:18 (robin/sparrow e.g.); Allan Testimony, Nov. 6 Transcript, at 18:17-21:12; P. Exh. 3, 6, 54.

548. Filters work especially well at blocking the most popular Web sites and the Web sites that are most likely to be accessed by a minor. For example, it is highly likely that every Web site that comes up in the first 50 results of a search engine query for "hard core porn" will be blocked by filtering products. Looksmart, for example, blocks the first 50 results for Google and Yahoo searches for "hard core porn." Search engines provide links directly to Web pages. Felten Testimony, Oct. 25 Transcript, at 32:1-20; Murphy Testimony, Nov 1 Transcript, at 194:6-196:6, 221:8-222:24; P. Exh. 2.

549. The emergence and widespread popularity of search engines, which have led most Internet users to go directly to Web pages through search engine links rather than by typing in a URL, combined with the Misleading Domain Name statute, has made it much less likely that a child will inadvertently access sexually explicit material if a filter is not being used, and even less likely if a filter is being used. P. Exh. 2.

550. Many search engines, including Google, provide a filtering feature for parents to use to block results that contain material not appropriate for children. If a parent so desires, a parent can therefore use both a search engine filter and a separate Internet content filter to restrict their children's access to the Internet.

b. Studies Prove the Effectiveness of Filters.

551. Numerous studies have been done over the years to measure the effectiveness of various Internet content filtering products. Evaluations of filter effectiveness usually focus on how accurate filters are at distinguishing between content that should and should not be blocked. "Underblocking" occurs when a filter fails to block content that is supposed to be blocked. "Overblocking" occurs when a filter blocks content that is not supposed to be blocked. Cranor Testimony, Oct. 24 Transcript, at 52:5-21; Allan Testimony, Nov. 6 Transcript, at 18:12-21:12.

552. To determine whether filters are an effective, alternative method of preventing children from accessing harmful to minors material, it is important to focus on underblocking rates, not overblocking rates, because underblocking rates measure how often filters actually block the material they intend to block – i.e., how often filters would block children from accessing inappropriate material. Overblocking simply

represents the potential consequences of the decision to prevent children from accessing inappropriate material. Cranor Testimony, Oct. 24 Transcript, at 52:22-53:6.

553. Although test results vary based on the methodologies used and products tested, the filtering studies have consistently determined that many filtering products are quite effective at blocking the vast majority of inappropriate material on the Web. The studies have found very low underblock rates and, for some products, very low overblock rates as well. More specifically, most studies indicate that the better filters have underblock rates of less than 10 percent, with some reporting underblock rates of less than 1 percent or in the 1-2 percent range. The overblock rates are generally even lower, with some studies finding there to be less than 1 percent overblocking. Cranor Testimony, Oct. 24 Transcript, at 55:8-23, 56:20-57:8, 58:7-25; P. Exh. 2; P. Exh. 3, at 1, 44, 45; P. Exh. 260; Allan Testimony, Nov. 6 Transcript, at 17:20-18:12.

554. These studies have also consistently concluded that filters perform especially well on material considered to be pornography, with some products blocking more than 95 percent of what they were supposed to block. Indeed, several studies have found that filters block virtually all material that is clearly pornography or erotica. Cranor Testimony, Oct. 24 Transcript, at 55:8-23; P. Exh. 3, at 44; Allan Testimony, Nov. 2 Transcript, at 232:3-17 Allan Testimony, Nov. 6 Transcript, at 17:20-18:12; Murphy Testimony, Nov. 1 Transcript, at 194:8-196:6.

555. For example, a study prepared by Etesting Labs for the Defendant determined that the four filtering products tested in the study correctly blocked an average of approximately 92 percent of the objectionable content (i.e., an 8 percent underblocking rate), and incorrectly blocked an average of 4 percent of non-

objectionable content (a 4 percent overblocking rate). Cranor Testimony, Oct. 24 Transcript, at 56:2-57:8. P. Exh. 3, at 1.

556. A second study conducted by Etesting Labs on three filtering products found that one product correctly blocked 95 percent of the adult material it was tested on, and that the other two products blocked 90 percent of that material. The overblocking rates for these products were all less than 1 percent. Cranor Testimony, Oct. 24 Transcript, at 58:7-15. P. Exh. 3, at 44, 45.

557. A study conducted for the Defendant by Corey Finnel analyzed the overblocking rates of three filtering products. Mr. Finnel found that the overblocking rates for those three products respectively were between 4.69 percent and 7.99 percent, between 5.25 percent and 11.03 percent, and between 6.92 and 9.36 percent, using a 95 percent confidence interval. Cranor Testimony, Oct. 24 Transcript, at 60:4-61:25.

558. Another major study was conducted for NetAlert and the Australia Broadcast Authority. That study measured the effectiveness of various filtering products at blocking a variety of different categories of content that parents might want to block, including pornography and erotica. The study found that some products, such as AOL's filter, blocked close to 100 percent of all pornography or erotica when the most restrictive setting (for children under the age of 12) was chosen. When a less restrictive setting (for 13 to 15 year-olds) was selected, the study similarly found that nearly 100 percent of the pornography and erotica were blocked. Cranor Testimony, Oct. 24 Transcript, at 62:1-19, 64:3-66:2.

559. Consumer Reports has also conducted reviews of the various filtering products available to parents. Their most recent study concluded that filters are very

good or excellent at blocking pornography, and that they block most, but not all, of that content. More specifically, Consumer Reports found that three products – from AOL, KidsNet and MSN – blocked practically every pornographic site that they tested, and that the least effective product they tested still blocked 88 percent of pornography. Cranor Testimony, Oct. 24 Transcript, at 70:9-22.

560. The methodology for the Consumer Reports study is not as well described as the methodology for many of the other studies. The Consumer Reports study is still informative, however, because Consumer Reports focuses its evaluations on the things that are most important to potential consumers, and provides information that is likely to be helpful to a parent deciding whether to use a particular product. Cranor Testimony, Oct. 24 Transcript, at 69:14-70:4.

561. Two separate reports commissioned by Congress – from the Commission on Child Online Protection and the National Research Council – have confirmed that content filters can be effective at preventing minors from accessing harmful materials online. Cranor Testimony, Oct. 24 Transcript, at 71:2-76:5; P. Exh. 6; P. Exh. 54.

562. The COPA Commission was established by Congress as part of the COPA legislation. The COPA Commission report concluded that although filters are not perfect, filters can be highly effective in directly blocking access to global harmful to minors content on the Web, as well as harmful to minors content available via newsgroups, email, and chat rooms. Cranor Testimony, Oct. 24 Transcript, at 71:22-72:9. P. Exh. 6, at 19.

563. The COPA Commission report also points out that content filters are flexible and that they can be customized based on an individual parent's preferences and

values. That flexibility is important, because it allows families to choose the kinds of restrictions that make sense for them. Cranor Testimony, Oct. 24 Transcript, at 73:20-74:8. P. Exh. 6.

564. The COPA Commission report also concluded that the time management and monitoring features in filtering products provide parents with additional effective tools to use to control their children's activities on the Internet. Those tools are particularly effective because they encourage parental involvement and can influence children's activities online. The COPA Commission noted that these features, like the content filtering aspects of filters, can be effective at controlling global Web content, as well as email and other non-Web communications on the Internet. Cranor Testimony, Oct. 24 Transcript, at 73:5-19; P. Exh. 6, at 34.

565. Overall, the COPA Commission report concluded that "voluntary approaches provide powerful technologies for families," especially when they are coupled with information to make these technologies and tools understandable for parents. Cranor Testimony, Oct. 24 Transcript, at 73:20-74:1; P. Exh. 6, at 39.

566. Congress also commissioned a study by the National Research Council to discuss the various issues raised by COPA, including the availability of other alternative methods of protecting children on the Internet. P. Exh. 54.

567. The National Research Council issued a lengthy report in 2005. The NRC's report's conclusions about filtering products were consistent with the findings of the COPA Commission. Specifically, the NRC report concluded that "for parents who want to restrict access to the Internet, filters can be highly effective in reducing the exposure of minors to inappropriate content," and that, "it is helpful to regard such

filtering as 'training wheels' for children on the Internet as they learn to make good decisions about what materials are and are not appropriate for their consumption." Cranor Testimony, Oct. 24 Transcript, at 75:15-76:3; P. Exh. 54, at 40.

568. Because all of these different studies have consistently reached the same conclusion – that there are many filtering products that are effective at blocking inappropriate content – it was not necessary for Dr. Cranor to conduct her own scientifically systematic study of the effectiveness of filtering products. Cranor Testimony, Oct. 24 Transcript, at 169:2-20.

569. The study conducted by Defendant in this case makes this point abundantly clear, because Defendant's study reaches findings that are consistent with and similar to the findings of all of the other filtering studies that have been conducted over the years. Specifically, as with all of the other studies, the Mewett/Stark study found that there are several filtering products that are highly effective and accurate at blocking sexually explicit material, especially the most popular Web content, and that many of the products have less than a 10 percent underblocking rate. Cranor Testimony, Oct. 24 Transcript, at 78:3-12, 81:1-17. P. Exh. 260.

c. Users are Satisfied with Filtering Products.

570. Real-world use of filtering products confirms what all of the various studies have concluded: filters can be an effective tool to restrict access to inappropriate content. For example, most parents using filters have expressed their satisfaction with their filtering products, and many believe the products are outperforming their expectations. Indeed, a study done for AOL found that 85 percent of parents are highly satisfied with their AOL Parental Controls products, and that 87 percent of the parents

find them easy to use. Cranor Testimony, Oct. 24 Transcript, at 83:7-11, 129:9-130:13; Murphy Testimony, Nov. 1 Transcript, at 222:25-223:20; P. Exh. 85, at 4.

571. Many government agencies use Internet content filters on their computers. Testimony from the Department of Justice itself confirms that filtering products are effective at blocking sexually explicit material, that underblocking and overblocking are rarely reported as problems, and that Internet users are very satisfied with the way they work. J. Exh. 1, ¶¶ 114-16, 124; Murphy Testimony, Nov. 1 Transcript, at 222:25-223:20, 229:16-230:10.

572. Filtering products are also widely used in most libraries and schools. Any school or library that receives federal funding for providing Internet access is required by a separate federal law, 21 U.S.C. § 9134; 47 U.S.C. § 254(h), to have filters installed and operating on all computers that are accessible by minors. Many states also require filters in schools and libraries. Taylor Testimony, Nov. 1 Transcript, at 169:15-17; Kirk Testimony, Nov.1 Transcript, at 86:2-9; Murphy Testimony, Nov. 1 Transcript, at 228:22 – 229:13; Smathers Testimony, Nov. 2 Transcript, at 17:13-16.

573. Children regularly test the effectiveness of filters in these real-world settings, by accessing thousands of Web pages per week from their school or school library computers. Many librarians are very satisfied with the products and the way they work. As one example, in a 2003 article, a Virginia librarian noted that during the first seventeen months of filtering in his library system, 2.4 million patrons surfed the Web, and there were only a mere 38 requests to unblock and 38 requests to block Web sites. P. Exh. 2.

574. Many schools are similarly satisfied with the protection and services offered by content filters. Taylor Testimony, Nov. 1 Transcript, at 177:3-10; Kirk Testimony, Nov.1 Transcript, at 90:7-91:12; 94:18-20; Smathers Testimony, Nov. 2 Transcript, at 23:25-24:17; P. Exh. 11, at 0005-0006.

575. Schools that use Internet content filters report minimal or non-existent underblocking and overblocking, despite the fact that students are regularly using the school computers to connect to the Internet. Kirk Testimony, Nov. 1 Transcript, at 91:18-93:18; Taylor Testimony, Nov. 1 Transcript, at 175:22-177:2; Smathers Testimony, Nov. 2 Transcript, at 23:11-24.

576. Overblocking is also not a significant problem for these schools because if a teacher believes a filter is filtering a Web page that should not be blocked, it only takes a minimal amount of time to alter the filter to permit access to the page. Kirk Testimony, Nov. 1 Transcript, at 88:18-20; Taylor Testimony, Nov. 1 Transcript, at 173:23- 174:6; Smathers Testimony, Nov. 2 Transcript, at 20:18-25, 21:23-22:7.

577. User satisfaction with filtering products is not surprising. Filtering products have improved over time and are now more effective than ever before, both in blocking intended material and in not blocking unintended material. That improvement is to be expected, because, as with all software, the filtering companies have addressed any problems with the earlier versions of the products in an attempt to make their products better. Cranor Testimony, Oct. 24 Transcript, at 81:18-82:10; Murphy Testimony, Nov 1 Transcript, at 194:6-196:6, 221:8-222:24.

578. Another reason the effectiveness of filtering products has improved is that many products now provide multiple layers of filtering. Whereas many filters once only

relied on blacklists or whitelists, many of today's products utilize blacklists, whitelists, and real-time, dynamic filtering to catch any inappropriate sites that have not previously been classified by the product. This multi-layered approach has increased the effectiveness of content filters and added an extra layer of protection, to ensure that even more content is blocked, if that is what a parent desires. Cranor Testimony, Oct. 23 Transcript, at 246:20-247:9; Cranor Testimony, Oct. 24 Transcript, at 81:18-82:4; Whittle Testimony, Oct. 31 Transcript, at 201:4-17.

579. Filtering products also cover more speech than ever before, in more languages, and offer more options to parents to customize the products to fit the individual circumstances of their families and children. Allan Testimony, Nov. 2 Transcript, at 208:17-21, 240:18-241:12; Whittle Testimony, Oct. 31 Transcript, at 200:2-16, 206:23-212:13; Murphy Testimony, Nov 1 Transcript, at 194:6-196:6, 221:8-222:24; P. Exh. 2.

580. There is a high level of competition in the field of Internet content filtering. That factor, along with the development of new technologies, has also caused the products to improve over time. Given that consumer demand has not diminished, it is likely that the products will continue to improve and become even more effective over time. Murphy Testimony, Nov. 1 Transcript, at 223:21-224:5; P. Exh. 2.

d. Defendant's Filtering Study Adds Nothing.

581. The filtering study conducted for Defendant by Mr. Mewett and Professor Stark is irrelevant because it did not examine the effectiveness of filters at blocking material that is "harmful to minors" or obscenity. As a result, the study does not address the central question of whether filters are as effective as COPA at blocking the speech

that is covered by COPA. Mewett Testimony, Nov. 7 Transcript, at 200:15-201:3, 201:22-202:6; Stark Testimony, Nov. 8 Transcript, at 165:20-25.

582. Defendant's study is irrelevant because in classifying the sample set of Web pages to be tested, Mr. Mewett did not consider whether the material on those pages had value "for minors." As a result, his classifications have no relationship to whether the speech would be covered by COPA. Mewett Testimony, Nov. 7 Transcript, at 201:18-21.

583. Defendant's study is irrelevant because it used a definition created by Mr. Mewett rather than the definitions created by filters, thus measuring the filters by standards they did not adopt or seek to meet. Mewett Testimony, Nov. 7 Transcript, at 202:10-16.

584. Defendant's study cannot be relied on for any overblocking statistics because it concluded that a filter had overblocked even when the filter was performing exactly as intended. This occurred because Mr. Mewett instructed the filters to block pages fitting categories such as violence and then reviewed the pages only for sexual content, such that if a page with violence was properly blocked, but did not contain sexual content, Mr. Mewett counted that page as being overblocked. Mewett Testimony, Nov. 7 Transcript, at 210:13-212:20.

585. Defendant's study cannot be relied upon because the category of "sexually explicit" sites contained an unknown number – of at least 183 sites – that were counted more than once. Mewett Testimony, Nov. 8 Transcript, at 5:16-7:8; P. Exh. 169, 170[2], 178.

[2] The database underlying Defendant's study is only available on a CD. The following instructions detail how to view these duplicate sites. Using the Access Database titled "Supplemental Revised Master

586. Defendant's study is flawed because it did not test any of the time management or monitoring features offered by filtering products. Mewett Testimony, Nov. 7 Transcript, at 202:17-21.

587. Defendant's study cannot be relied upon because the qualifications of the people who did the categorizations of the pages used in the test were unknown, and their reliability un-established. Mewett Testimony, Nov. 7 Transcript, at 207:19-210:2.

588. Defendant's study cannot be relied upon because the categorizations used in the test often appeared irrational. P. Exh. 177, 180-182; Mewett Testimony, Nov. 7 Transcript, at 224:16-233:15, Nov. 8 Transcript, at 10:9-26:22; Compare Nov. 7 Transcript, at 235:21-236:12 with Nov. 8 Transcript, at 22:15-24:4.

589. Defendant's study cannot be used to generalize because it contained a number of statistics that represented very small sample numbers. For example, the analysis of "free, foreign" Web pages was based on fewer than 50 Web pages. D. Exh. 83, ¶38; D. Exh. 79; P. Exh. 169[3]; Mewett Testimony, Nov. 8 Transcript, at 31:16-34:24; Stark Testimony, Nov. 8 Transcript, at 170:13-171:5.

590. Defendant's study cannot be used to generalize because it contained a number of statistics that represented very small sample numbers. For example, the analysis of "domestic underblocked" pages included only 4 of 10 pages in the Google

---

Database" on the CD that contains Plaintiff Exhibit 170, a menu will appear with six tables. Each table contains data that Mr. Mewett collected from the source mentioned in the table's title. To see an example of duplicate "sexually explicit" sites, open the table labeled "Wordtracker," which contains the URLs retrieved from searches of words from the source Wordtracker. With the computer's mouse, right-click in the column that is labeled "URL" and select "Sort Ascending." Scroll about half way down the database, to see approximately 190 URLs with the same domain "destinationxxx."

[3] Using Attachment C ("Free Foreign 5F Database") on the CD that contains Plaintiffs' Exhibit 169, a menu will appear with six tables. By opening any of these tables the number of unique Ids located in the "Id" column can be counted. By totaling the unique Ids from all the tables, the number of Web pages used for the analysis of "free, foreign" Web pages is illustrated.

index and 13 of 32 pages in the MSN index. D. Exh. 72; P. Exh. 169; Stark Testimony, Nov. 8 Transcript, at 166:16-168:21.

591. One portion of Defendant's study analyzed a random set of Web pages derived from the Google and MSN indexes. Mewett Testimony, Nov. 8 Transcript, at 203:22-25; D. Exh. 62, 82. The portion of Defendant's study that relied on a random set of Web pages derived from the Google and MSN indexes cannot be used to determine how successful filters are when people are actually accessing pages on the Web because people do not access pages randomly and there is no evidence that anyone but Mr. Mewett ever viewed any of those pages. Mewett Testimony, Nov. 8 Transcript, at 204:1-10; 205:6-17.

592. One portion of Defendant's study analyzed Web pages derived from the Yahoo, MSN, and AOL random search queries. D. Exh. 62, 82. The portion of Defendant's study that relied on Web pages derived from the Yahoo, MSN, and AOL random search queries cannot be used to determine how successful filters are when people are actually accessing pages on the Web because there is no evidence the searches used were ever done by a human being or, even if they had been done by a human being, that the Web pages returned when Mr. Mewett searched would be the same as those returned when another person did the search. Mewett Testimony, Nov. 8 Transcript, at 205:18-206:3.

593. One portion of Defendant's study analyzed Web pages derived from 650 of the most popular searches as reported by the Web site WordTracker. This portion utilized searches actually done by actual people. D. Exh. 62, 83.

594. When Defendant's study analyzed the success of filters at blocking Web pages returned as a product of actual searches of popular terms (as reported by WordTracker), the filters tested were successful at blocking Mr. Mewett's "sexually explicit" pages at the following rates:

AOL Mature Teen	98.7%
MSN Pornography	97.3%
MSN Teen	97.4%
Content Protect default	92.5%
Content Protect custom	91.9%
CyberPatrol custom	96.1%
CyberPatrol default	98.6%
CyberSitter Custom	97.1%
McAfee Young Teen	97.2%
Net Nanny Level 2	87.4%
Norton default	90.1%
Norton custom	89.8%
Verizon	95.6%
8e6	96.6%
SafeEyes	98%

P. Exh. 260; P. Exh. 170.[4]

595. The majority of the filters tested in Defendant's study blocked most of the sexually explicit pages specifically identified by Defendant. D. Exh. 88; P. Exh. 168-170[5]; Mewett Testimony, Nov. 8 Transcript, at 28:19-21.

596. Out of the 11,100 Web pages from the Google index categorized by Mr. Mewett, the number of sexually explicit Web pages that were also domestic and not blocked by the AOL filter was 4, or 00.036%. P. Exh. 170.[6]

[4] By using the Access Database titled "Supplemental Revised Master Database" on the CD that contains Plaintiffs' Exhibit 170, a menu will appear with six tables. Within the "Wordtracker" table there are columns indicating the successful blocks of "sexually explicit" sites used to calculate these percentages. For example, the column, "AOL Mature Teen Blocked" indicates when a URL was blocked by the AOL filter when on the Mature Teen setting.

[5] Using the "Supplemental Revised Master Database" on Plaintiffs' Exhibit 170, search for the Id numbers identified at the top of each page identified in Defendant's Exhibit 88 in the appropriate table. By scrolling across the database if a URL was blocked, it is noted in the appropriate column.

597. Out of the 39,999 Web pages from the MSN index categorized by Mr. Mewett, the number of sexually explicit Web pages that were also domestic and not blocked by the AOL filter was 13, or 00.033%. P. Exh. 170.[7]

598. Out of the 10,201 Web pages from the three random search query analyses categorized by Mr. Mewett, the number of sexually explicit Web pages that were also domestic and not blocked by the AOL filter was 5, or 00.05%. P. Exh. 170.[8]

599. Out of the 6,850 Web pages from the WordTracker search analysis categorized by Mr. Mewett, the number of sexually explicit Web pages that were also domestic and not blocked by the AOL filter was 11, or 00.16%. P. Exh. 170.[9]

9. Filters Cannot be Circumvented.

600. One of the features of filtering programs that adds to their effectiveness is that they have built-in mechanisms to prevent children from bypassing or circumventing the filters, including password protection and other devices to prevent children from uninstalling the product or changing the settings. Some products even have a tamper detection feature, by which they can detect when someone is trying to uninstall or disable the product, and then cut off Internet access altogether until it has been properly reconfigured. Cranor Testimony, Oct. 24 Transcript, at 86:19-87:25; Felten Testimony, Oct. 25 Transcript, at 37:05-38:07; Murphy Testimony, Nov. 1 Transcript, 216:12-217:18; Whittle Testimony, Oct. 31 Transcript, at 215:7-14; P. Exh. 2; P. Exh. 86.

---

[6] Using the "Supplemental Revised Master Database" on Plaintiffs' Exhibit 170, open the table labeled "Google." At the top, click "Records" and then "Advanced Filter." Sort in descending order by "5f" which is Mewett's "sexually explicit" category, then by "Hosting Country," and lastly by "AOL MatureTeen Not Blocked." After applying the Filter, by looking at the corresponding columns, the domestic URLs not blocked by AOL Mature Teen can be counted.

[7] Repeat the process described in Footnote 5 using the table labeled "MSN URL."

[8] Repeat the process described in Footnote 5 using the tables labeled "MSN Query," "AOL Query," and "Yahoo Query," and adding the totals.

[9] Repeat the process described in Footnote 5 using the table labeled "Wordtracker."

601. Filtering companies actively takes steps to make sure that children are not able to come up with ways to circumvent the filters. Filtering companies actively monitor the Web to identify any information about circumventing filters, and whenever possible circumvention methods are discussed on the Web, the filtering companies respond by putting in extra protections to make sure that those methods do not succeed with their products. Cranor Testimony, Oct. 24 Transcript, at 86:19-87:21; Felten Testimony, Oct. 25 Transcript, at 38:08-39:01.

602. It is difficult for children to circumvent filters. Very few minors have the technical ability and expertise necessary to circumvent filtering products either by disabling the product on the actual computer or by accessing the Web through a proxy or intermediary computer to avoid a filter on the minor's computer. Cranor Testimony, Oct. 24 Transcript, at 86:19-21; Felten Testimony, Oct. 25 Transcript, at 36:06-40:04; Murphy Testimony, Nov. 1 Transcript, 216:12-217:18; Whittle Testimony, Oct. 31 Transcript, at 215:7-14; Allan Testimony, Nov. 2 Transcript, at 244:9-15.

603. Accessing the Web through a proxy or intermediary computer will not enable a minor to avoid a filtering product that analyzes the content of the Web page requested, in addition to where the page is coming from. Any product that contains a real-time, dynamic filtering component cannot be avoided by use of a proxy, whether the filter is located on the network or on the user's computer. Felten Testimony, Oct 25 Transcript, at 38:08-39:24.

604. For certain ISP filtering products, like AOL's product, broadband users are required to download additional software to ensure that the filter works on all Internet connections. It takes about one minute to download and install that software

through a simple point and click process that AOL walks the user through. Cranor Testimony, Oct. 24 Transcript at 30:20-32:22; P. Exh. 86 at 15-22.

605. Filters cannot be circumvented through use of a laptop computer. Filters work on both desktop and laptop computers. Thus, if filtering software is installed on a laptop computer, it can filter Internet content wherever the computer is used, even if a child takes it outside the home. Cranor Testimony, Oct. 24 Transcript at 88:22-23; Murphy Testimony, Nov. 1 Transcript, at 214:14-22.

606. Filters cannot be circumvented simply because a family has more than one computer in the home. Filtering products are designed to work if a family has more than one computer, and they can be installed on multiple computers in a home. Cranor Testimony, Oct. 24 Transcript at 88:24-88:1; Murphy Testimony, Nov. 1 Transcript, at 214:1-10.

10. Filtering Products are Widely Used by Parents.

607. Many people are using the parental control tools offered by content filtering products. Although the exact number of people using filters is difficult to determine, a recent study by PEW Internet Research found that approximately 54 percent of Internet-connected families with teenagers are using filters. That figure represents a 65 percent increase from a prior PEW study done four years earlier, indicating that more and more families are using filtering products now. Cranor Testimony, Oct. 24 Transcript at 88:2-5, 90:3-13.

608. PEW Internet Research is a research organization that has conducted a number of studies about the use of the Internet. Studies by PEW are relied upon by

experts in the field, and the particular methodology utilized in the PEW study referenced in the prior paragraph was reliable. Cranor Testimony, Oct. 24 Transcript at 88:12-89:8.

609. It is not possible to know why certain families do not use filters. Studies have been conducted to determine why parents do or do not choose to use filters. The number one reason provided by parents for why they do not use filters is that they do not feel like they need to use filters because they trust their children and do not see a need to actually block any content, preferring instead just to check up on their children's Internet activities. Cranor Testimony, Oct. 24 Transcript at 90:14-91:2, 133:20-134:4; Whittle Testimony, Oct. 31 Transcript, at 219:5-15; P. Exh. 85, at 4, 49.

610. More specifically, a study done for AOL found that 60 percent of parents were not using filters because they trust their children and do not see the need to use filters. Cranor Testimony, Oct. 24 Transcript at 133:20-134:4; Whittle Testimony, Oct. 31 Transcript, at 219:5-15; P. Exh. 85, at 49.

611. Filtering products are essentially just another type of security software for use by computer owners. Statistics show that other highly effective security software products, such as anti-virus software, are not used by all computer owners for a variety of similar reasons. The percentage of users utilizing filtering products is not unexpected and is in fact a higher percentage of use than many analysts would have expected. P. Exh. 2.

11. Internet Content Filters Are Available for Use on New Technologies.

612. Content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as mobile phones, personal digital assistants ("PDAs") such as the Blackberry, portable

audio/video players such as the iPod, and game consoles. Many of these devices are essentially computers, packaged differently, and with differing user interfaces. Felten Testimony, Oct. 25 Transcript, at 19:15-24.

613. There has not previously been a market demand for content filtering on mobile devices. Just as widespread use of traditional computers created a market for filtering products on those devices, as mobile phones have started having broadband-like capabilities, it is reasonable to expect that there will be a market for mobile filtering products. Sena Testimony, Nov. 2 Transcript, at 33:22-35:04.

614. Although many devices are now capable of accessing the Internet, a very small percentage of individuals with such devices are actually using them to access the Internet. Ryan Testimony, Nov. 6 Transcript, at 38:9-25.

615. Content filtering technology can be used on these alternative, non-PC devices. There are no fundamental barriers to the feasibility of content filtering on the devices. Filtering for alternate Internet-capable devices poses essentially the same technological issues as filtering on ordinary computers. It is possible to provide the same type and quality of content filtering for such devices as for ordinary computers. Felten Testimony, Oct. 25 Transcript, at 19:25-20:21; 24:18-25:03. Sena Testimony, Nov. 2 Transcript, at 33:04-0637:07-25, 60:25-61:13; P. Exh. 70; Murphy Testimony, Nov. 1 Transcript, at 204:4-205:3, 233:13-234:4; Allan Testimony, Nov. 6 Transcript, at 9:16-10:9.

616. Some alternative devices, such as certain PDAs and portable music players like the iPod, cannot receive content directly over the Internet, but can only receive it via a wired connection to a personal computer, after the content has been

downloaded to the personal computer first. For these devices, the content will already have been subjected to the personal computer's Internet content filter, if the user has chosen to use a filtering product, so an additional filtering product for these devices is not necessary. P. Exh. 13 at 19.

617. Filtering technology can be implemented for users of other alternative devices in several ways. One approach is to perform content filtering in the network, not on the device itself, much as is done for most ISP-based filters for personal computers. In this approach, equipment run by the network provider (e.g., the cellular network for a mobile phone) would observe, inspect, and filter network traffic in transit between the alternative device and the rest of the Internet. Felten Testimony, Oct. 25 Transcript, at 24:06-25:03.

618. Another approach is to run filtering software on the device itself. Devices such as mobile phones are really just small computers, which are capable of running the same types of software applications that desktop computers can run. The creator of a filtering program for desktop computers can simply take that program and modify it slightly so that it works on an alternative device. Felten Testimony, Oct. 25 Transcript, at 20:22-21:08.

619. Some alternative devices have less memory or slower processors than desktop computers. Less capable devices may have difficulty running some application programs. Due to the rapid and fairly predictable improvements in the capacity of memories and discs and the speed of processors, this state of affairs will only be temporary, and it is very likely that in the near future, almost all alternative devices will be able to run almost all applications that are used on personal computers today,

including anti-virus software and content filtering software. Felten Testimony, Oct. 25 Transcript, at 21:09-22:10.

620. Yet another approach to implementing filtering for alternative devices is to route a user's content requests through a proxy. When a proxy is in use, and the browser needs to retrieve a file via HTTP, the browser does not request the file directly from the server that is offering it. Instead, the browser contacts the proxy and tells the proxy the URL of the file the browser wants. The proxy then contacts the server, retrieves the designated file, and passes the file back to the browser. Because the proxy handles every file (i.e., every page, image, etc.) that the browser gets, the proxy can filter the files to remove specified material, such as harmful to minors material. Felten Testimony, Oct. 25 Transcript, at 22:11-24:05.

621. Accessing the Web via a proxy, rather than accessing servers directly, makes no material difference in the amount of memory, computational power, or other resources that a mobile device will use. There is no noticeable difference for the user. P. Exh.13, at 21.

622. Mobile devices can, and often do, use HTTP proxies. The filtering proxy can be a computer (or bank of computers) anywhere on the Internet – it might be provided by a mobile phone company, by a filtering company, or by anyone else. P. Exh. 13, at 21.

623. Filtering for alternative Internet access devices can be implemented transparently to the user, so the user's experience of using the device would be the same as it would be if the filter were not present (except for the unavailability of filtered content). The user interface for enabling, disabling, and controlling the filter could be

essentially the same as on an ordinary computer. Sena Testimony, Nov. 2 Transcript, at 49:13-52:02; P. Exh. 13 at 22; P. Exh. 70.

624. Several vendors, including large, experienced software companies, currently offer content filtering products for alternative devices. Examples include products offered by Ace*comm, Bytemobile, Blue Coat, Cisco, and RuleSpace, to name a few. Felten Testimony, Oct. 25 Transcript, at 25:04-20. Sena Testimony, Nov. 2 Transcript, at 33:04-06, 60:07-14; P. Exh.13, at 22-23; P. Exh. 70; Allan Testimony, Nov. 2 Transcript, at 223:2-23.

625. The companies that provide filtering products for traditional computers could also relatively easily modify their products for use on alternative devices. Many do not currently have products available for use on alternative devices because, given the recent emergence of such devices, there has not yet been a market demand for such products. Several of these companies are now considering whether to provide such a product, and once the demand is there, they are likely to provide such a filtering product. Allan Testimony, Nov. 6 Transcript, at 9:16-10:9; Murphy Testimony, Nov. 1 Transcript, at 204:4-205:3, 233:13-234:4.

626. Several major mobile phone carriers, including Cingular, Sprint-Nextel, and Alltel, are presently offering parental controls features, including some content filtering, to enable parents to control their children's access to the Internet. These tools enable parents so desiring to, among other things, limit the Web content accessible through the phones to pre-selected, child friendly material, and prevent their children from using chat rooms, instant messaging, text messaging, email, purchasing any file downloads or having any access to the Internet at all. Felten Testimony, Oct. 25

Transcript, at 25:22-26:02; Ryan Testimony, Nov. 6 Transcript, at 30:20-36:19; Allan Testimony, Nov. 2 Transcript, at 223:2-23.

627. Mobile carriers are actively soliciting bids for the provision of mobile content filtering services. The top five mobile carriers in the United States, Cingular, Verizon Wireless, T-Mobile, Sprint, and Alltel, are all soliciting bids. Sena Testimony, Nov. 2 Transcript, at 56:19-57:09.

628. Ace*Comm offers a mobile filtering product called Parent Patrol. Ace*Comm created Parent Patrol because it identified a market need for mobile filtering software. Sena Testimony, Nov. 2 Transcript, at 33:22-35:04.

629. Parent Patrol enables parents to filter the Web content their children access through their mobile devices. Parents can choose to block particular categories of content, such as pornography or content pertaining to drugs or gambling. Parents can also create a "black list" of specific websites that their children's phones will not be able to access, and a "white list" of specific websites that their children's phones will always be able to access. Parents can additionally restrict the time of day and number of hours their children use their cell phones to access the Web. Sena Testimony, Nov. 2 Transcript, at 35:05-20, 39:05-40:16.

630. Running the Parent Patrol filtering program causes no delay noticeable to the user regarding how long it takes to view a requested web page. Sena Testimony, Nov. 2 Transcript, at 55:05-06.

631. Parent Patrol also enables parents to place restrictions on other aspects of cell phone use, such as voice calls and text messaging. Sena Testimony, Nov. 2 Transcript, at 35:05-20

632. Parent Patrol is available for purchase by mobile network operators. Parent Patrol is installed on the mobile carrier's network. Because it is installed on the mobile carrier's network, it is handset independent. That is to say, it can be applied to any kind of mobile devices, including cell phones, blackberries, and wireless-enabled laptops. Sena Testimony, Nov. 2 Transcript, at 35:21-36:06.

633. A North American mobile carrier has accepted a contract to implement Parent Patrol. The contract is for the voice services aspect of Parent Patrol, and was set to commence in November 2006. The same carrier is considering implementing the data content filtering elements of Parent Patrol in early 2007. Sena Testimony, Nov. 2 Transcript, at 59:06-60:04.

634. The major U.S. mobile carriers have agreed to abide by industry guidelines concerning Internet access and wireless content. Those guidelines require the carriers, among other things, to: (1) classify content into at least two categories – content available for all users and restricted content available for those over 18 years-old or those whose parents have specifically authorized access; (2) not provide access to restricted content until the carrier has deployed controls to restrict access to such material; (3) provide controls to restrict access to restricted content; and (4) consistent with each company's business plans, provide users with access to content filters that can restrict all Internet content not previously classified by the carrier. Ryan Testimony, Nov. 6 Transcript, at 43:4-10; Sena Testimony, Nov. 2 Transcript, at 33:22-35:04.

635. Parents who are especially concerned about their children accessing inappropriate Web content through their cell phones can give their children cell phones that do not connect to the Internet, or a cell phone, such as the Firefly phone, which is

especially designed for kids and offers a range of parental control features. Felten Testimony, Oct. 25 Transcript, at 26:02-17.

12. Defendant's Attempts to Argue that Filters are Not an Effective Less Restrictive Alternative Should be Rejected.

a. Professor Neale's Testimony.

636. Defendant's purported filtering expert, Professor Stephen Neale, has no opinion regarding whether Internet content filters are more or less effective than COPA in preventing minors from gaining access to sexually explicit content. Testimony of Stephen Neale, Nov. 9 Transcript, 69:4-8.

637. Professor Neale's expert report and testimony is incomplete and unreliable. Professor Neale's expert report and testimony exclusively address linguistic functions and limitations of filters. Some filtering companies utilize non-linguistic classification methods that are not discussed in Professor Neale's report. Professor Neale conceded that an evaluation of the overall effectiveness of filters would be incomplete without including an analysis of non-linguistic functions. Professor Neale's report and testimony address only one specific component of content filtering, and do not purport to provide a full conclusion about the effectiveness of filters in preventing minors from seeing sexually explicit content. Neale Testimony, Nov. 9 Transcript, 69:9-72:13.

638. Professor Neale has no expertise or training in the software and hardware associated with Internet content filtering. Neale Testimony, Nov. 9 Transcript, at 79:1-4.

639. Prior to being retained as an expert by the Defendant, Professor Neale had never conducted any research or published any work addressing the World Wide Web or

the capabilities of Internet content filters. Neale Testimony, Nov. 9 Transcript, at 79:5-14.

640. Professor Neale does not purport to offer an expert opinion regarding any of the content in sections 3 and 4 of his expert report. Neale Testimony, Nov. 9 Transcript, at 80:10-18.

641. Professor Neale does not purport to offer an expert opinion about the effectiveness of methods of circumventing content filters. Neale Testimony, Nov. 9 Transcript, at 81:17 to 82:1.

642. Professor Neale conducted no tests of the effectiveness of filtering software in blocking sexually explicit content. Neale Testimony, Nov. 9 Transcript, 80:19 to 81:2.

b. Dr. Eisenach's Testimony.

643. Defendant's purported filtering expert Dr. Jeffrey Eisenach was offered as, and admitted as, an expert solely "on the Internet and its impact on markets and public policy." Eisenach Testimony, Nov. 13 Transcript, at 72:02-10.

644. Areas beyond Dr. Eisenach's expertise included: rates of underblocking and overblocking (Eisenach Testimony, Nov. 13 Transcript, at 110:18-21; 113:02-12); whether ICF software is an effective and viable option for families who wish to protect their children from sexually explicit material (Eisenach Testimony, Nov. 13 Transcript, at 157:16-22; 159:04-06); cellphone filtering technology (Eisenach Testimony, Nov. 13 Transcript, at 164:18-22); and the technological overlap between home and enterprise ICF (Eisenach Testimony, Nov. 13 Transcript, at 161:04-24.). While Dr. Eisenach

makes statements about these subjects in his written expert report, they are beyond his expertise and should be disregarded.

645. Dr. Eisenach's rebuttal report was admitted for the limited purposes of proving that it was generated and distributed, and that it constitutes Dr. Eisenach's opinion and limits his opinion in rebuttal. Eisenach Testimony, Nov. 13 Transcript, at 156:12-15.

646. Areas in which Dr. Eisenach's testimony was explicitly *not* received for its truth include: the percentage of parents who use ICF software (Eisenach Testimony, Nov. 13 Transcript, at 85:14-19; 87:25-88:02); Internet users' evaluations of the effectiveness of ICF software (Eisenach Testimony, Nov. 13 Transcript, at 116:15-25); frequency of repeat purchases of ICF software (Eisenach Testimony, Nov. 13 Transcript, at 131:06-14; 132:11-13); factors affecting consumer security suite purchasing decisions (Eisenach Testimony, Nov. 13 Transcript, at 148:06-19); factors affecting consumer ISP or broadband selection decisions (Eisenach Testimony, Nov. 13 Transcript, at 149:14-150:03, 150:20-151:04); supplier incentive to create and market ICF products (Eisenach Testimony, Nov. 13 Transcript, at 152:03-153:11); supplier revenue potential from ICF software (Eisenach Testimony, Nov. 13 Transcript, at 152:03-153:11); conditions in the market for ICF software that effect producer incentive to invest in creating and marketing ICF software (i.e., high fixed costs, small market size, competitive imperative to differentiate products, and ability of consumers to evaluate product quality) (Eisenach Testimony, Nov. 13 Transcript, at 141:25-145:04); incentives of producers of residential filtering products to seek to improve these products (Eisenach Testimony, Nov. 13 Transcript, at 152:03-153:11); whether the technological skills of parents are a factor in

ICF software use rates (Eisenach Testimony, Nov. 13 Transcript, at 108:23-109:05); ability of consumers to distinguish high quality products from low quality products (Eisenach Testimony, Nov. 13 Transcript, at 141:25-145:04); and the percentage of households with minor children using filtering software. Eisenach Testimony, Nov. 13 Transcript, at 83:13-15, 84:14-19.

647. The evidence in the record establishes that the market for filtering products is not broken. Producers of ICF filtering software continue to invest in creating new products and updating existing ones. Eisenach Testimony, Nov. 13 Transcript, at 186:19-21, 187:09-14. Manufacturers of ICF software believe there is sufficient profit to be earned to justify the cost of developing new products. Eisenach Testimony, Nov. 13 Transcript, at 187:25-188:03.

648. High fixed costs and low marginal costs are characteristic of all software products, not just ICF software. Eisenach Testimony, Nov. 13 Transcript, at 183:10-15.

649. Dr. Eisenach did not account for the effect of non-filtering based parental control software tools such as parental reporting, time management, monitoring and application blocking tools in deterring minors from accessing sexually explicit material online. Eisenach Testimony, Nov. 13 Transcript, at 166:17-167:04.

650. Although Dr. Eisenach stated what he believes to be the percentage of Internet-connected households with children that use filtering software, there is no evidence in the record supporting his statement and his statement was not admitted for its truth. Eisenach Testimony, Nov. 13 Transcript, at 83:13-15, 84:14-19, 87:25-88:02; 94:22-95:10.

651. In his expert report, Dr. Eisenach references survey data that he claims addresses the portion of households with minor children that use filtering software. At trial, it was clarified that the survey data referenced by Dr. Eisenach is not being used (or admitted) for its truth, but merely to indicate the type of surveys that someone in his position would rely upon, to prepare Dr. Eisenach to testify regarding his view of the state of the market. Eisenach Testimony, Nov. 13 Transcript, at 82:12-83:20.

652. Dr. Eisenach is not qualified to opine on whether ICF software is an effective and viable option for families who wish to protect children from sexually explicit material online. Eisenach Testimony, Nov. 13 Transcript, at 157:16-22; 159:04-06.

653. While Dr. Eisenach in his report makes statements regarding the degree to which ICF software can effectively be used by consumers, this subject is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

654. Although Dr. Eisenach makes statements regarding why families may choose not to use ICF software, such issues are beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

655. In addition, Dr. Eisenach testified that he did not consider the many reasons families may choose not to use ICF software. Eisenach Testimony, Nov. 13 Transcript, at 164:23-166:15. Reasons he failed to consider include: opposition to censorship; prohibiting Internet access entirely; or the belief that education, monitoring,

stationing the computer in a common area of the home, limiting children's online experience to times when the parent can participate, or the use of non-filtering parental control software – individually or in combination – is an effective means of limiting exposure to adult material online. Eisenach Testimony, Nov. 13 Transcript, at 164:23-166:15.

656. There is no evidence in the record supporting Dr. Eisenach's statements on the subject of computer software usability. Eisenach Testimony, Nov. 13 Transcript, at 100:16-18; 103:18-23. In addition, the topic is beyond the scope of the expertise for which he was offered as an expert at trial, or for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

657. There is no evidence in the record that the number of consumer complaints regarding ICF software differs from the number of complaints about other software products. Eisenach Testimony, Nov. 13 Transcript, at 169:02-06.

658. Although Dr. Eisenach makes statements in his report suggesting there are deterrents to the effective use of filtering software by parents, the topic is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03. For example, the Court specifically held that Dr. Eisenach is not qualified to opine on whether parents are deterred from using ICF software as a consequence of underblocking and overblocking rates. Eisenach Testimony, Nov. 13 Transcript, at 110:18-21; 113:02-12.

659. To the extent that purchasers of ICF software do not know the quality of the product they purchase until they install and use it, this condition is common to some extent to all software. Eisenach Testimony, Nov. 13 Transcript, at 170:16-21.

660. Dr. Eisenach relied on research by Dr. Akerlof in forming his Lemon problem analysis. A condition identified by Dr. Akerlof as the source of the Lemon problem in the market for used cars is that individual cars, which have the identical make, model and year, may be of differing quality. Eisenach Testimony, Nov. 13 Transcript, at 171:18-22. In comparison, since all copies of an ICF software program are identical in quality, the market for ICF software does not share with the market for used cars the condition that each unit may be of different quality. Eisenach Testimony, Nov. 13 Transcript, at 172:02-173:03.

661. There is no evidence in the record regarding the size of the market for ICF software that supports Dr. Eisenach's statement on the subject. Eisenach Testimony, Nov. 13 Transcript, at 143:02-06.

662. There is no evidence in the record to support the statements Dr. Eisenach makes in his report regarding projected changes in home use of personal computer ICF software.

663. There is no evidence in the record addressing whether consumers making purchases of ICF software do so without assessing the quality of the product. While Dr. Eisenach makes statements regarding this subject in his expert report, no testimony on the subject was elicited at trial. In addition, the topic is beyond the scope of the expertise for which he was offered as an expert at trial, or for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

664. There is no evidence in the record addressing whether, when consumers of ICF software use a product, they are unable to determine whether the product is good or bad. Testimony from Dr. Eisenach alleging that consumers "have a difficult time evaluating the quality of ICF software" was received as reliance and not for its truth. Eisenach Testimony, Nov. 13 Transcript, at 141:25-145:04.

665. Dr. Eisenach alleges that there is a Lemon problem in the market for ICF software, citing the work of Dr. Akerlof. In his analysis of the ICF market, Dr. Eisenach did not acknowledge the effect of guarantees and free trials to alleviate any asymmetry of information between producers and consumers. Eisenach Testimony, Nov. 13 Transcript, at 176:16-19. Dr. Akerlof specifically identified guarantees as an institution which arises to counteract the effect on a market of asymmetry of information between producers and consumers – i.e., to eliminate that market problem. Eisenach Testimony, Nov. 13 Transcript, at 176:08-15. Dr. Eisenach did not analyze which ICF products offer guarantees or free trials, though he admitted that "many of them I believe do." Eisenach Testimony, Nov. 13 Transcript, at 177:08-178:08.

666. Product reviews are another institution which arises to circumvent a potential Lemon problem in a given market. Eisenach Testimony, Nov. 13 Transcript, at 180:09-12. Many sources of product reviews of ICF software are available: online review websites, general computing magazines, and general sources such as Consumer Reports. Eisenach Testimony, Nov. 13 Transcript, at 180:20-82:09. Consumer Reports, for example, does an excellent job of simplifying complex information and in generating a rating system that is understandable to consumers of ICF software. Eisenach Testimony, Nov. 13 Transcript, at 182:10-16.

667. There is no evidence in the record regarding whether producers of high quality ICF products are unable to obtain full value for the products they produce. Similarly, there is no evidence in the record regarding whether consumers are willing to pay the cost of producing higher quality ICF products.

668. While Dr. Eisenach makes statements in his report regarding the habits of broadband users, no trial testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

669. While Dr. Eisenach makes statements in his report regarding the number of cell phones that have the ability to access the Internet, no testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03. Likewise, while Dr. Eisenach states in his report that adult content providers are actively pursuing the cellphone market, no testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

670. While Dr. Eisenach makes statements in his report regarding technical aspects of ICF software filters, no trial testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial,

and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

671. While Dr. Eisenach makes statements in his report regarding issues of parental knowledge of ICF software, maintenance and updating frequency, as well as the "socially acceptable" responses to a survey seeking ICF usage information, no trial testimony was elicited from him on these subjects, and they are beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

672. While Dr. Eisenach made statements in his report and in trial testimony regarding issues of ease of installation, configuration, updating and use of ICF software, these subjects are beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

673. While Dr. Eisenach makes statements in his report regarding consumer experiences with ICF software, including the effectiveness of customer support call lines, no trial testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03. To the extent his report cites to surveys claiming to collect the comments of individual consumers, such data constitutes inadmissible hearsay. In any case, Dr. Eisenach is not qualified to evaluate the reliability of survey data.

674. While Dr. Eisenach makes statements in his report regarding a persistent parent's ability to prevent a child from viewing sexually explicit material, no trial testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

675. While Dr. Eisenach makes statements in his report regarding the degree of technological sophistication required of parents to install and use ICF software, and the costs associated with ICF software, no testimony was elicited from him on these subjects, and they are beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

676. While Dr. Eisenach makes statements in his report regarding the penetration of alternative Internet access devices ("IADs"), no trial testimony was elicited from him on this subject, and it is beyond the scope of the expertise for which he was offered as an expert at trial, and for which he has qualifications to serve as an expert. Eisenach Testimony, Nov. 13 Transcript, at 72:02-03.

B. Defendant Failed to Prove that the Other Less Restrictive Alternatives are not Effective Alternatives.

1. Prosecute Existing Laws.

a. Obscenity Prosecutions.

677. Defendant is not prosecuting Web pages that fit his definition of obscenity. There have been very few prosecutions for obscenity over the past ten years. From 2000-2005, Defendant initiated fewer than twenty prosecutions for obscenity.

Since 2005, Defendant has initiated fewer than ten prosecutions for obscenity. P. Exh. 166, p. 0012-13 (Interrogatory 16); J. Exh. 1, at ¶¶ 122, 123; P. Exh. 54, at 0117, 0141-0143, 0229-0233.

678. That Defendant is not prosecuting Web pages that fit his definition of obscenity was demonstrated in the instant case. Defendant's experts came across Web pages that meet Defendant's definition of obscenity, including bestiality and violence against women, yet Defendant has not initiated prosecution. Mewett Testimony, Nov. 8 Transcript, at 7:9-10:8; P. Exh. 179; D. Exh. 88, at 10; P. Exh. 166, at 0012-13 (Interrogatory 16).

679. Much of the material that might be considered harmful to minors and prosecutable under COPA would also be considered obscene and is, therefore, already prosecutable under existing laws. P. Exh. 161; P. Exh. 163; P. Exh. 164; P. Exh. 165; P. Exh. 166; P. Exh. 167; P. Exh. 54, at 0231-0233.

680. Defendant has admitted that the government's interest in protecting children from harmful to minors material could be addressed through vigorous enforcement of other existing criminal statutes. P. Exh. 55.

681. Both the COPA Commission report and the National Research Council report concluded that the government's interest in protecting children from harmful to minors material could be addressed through vigorous enforcement of other existing criminal statutes such as the obscenity laws. The COPA Commission report expressly concluded that it is "imperative that government allocate increased resources to law enforcement" to prosecute existing laws and that "an aggressive effort to address illegal,

obscene material on the Internet will also address the presence of harmful to minors material." P. Exh. 6, at 0039, at 0043; P. Exh. 54, at 0241.

682. Defendant did not introduce any evidence at trial establishing that more vigorous enforcement of existing obscenity laws would not address the government's interest in protecting children from harmful to minors material.

b. Misleading Domain Name Prosecutions.

683. The Misleading Domain Name statute (18 U.S.C. § 2252B) prohibits the use of misleading domain names by Web sites and prevents Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them. J. Exh. 1, at ¶ 123; P. Exh. 54, at 0136-0139.

684. Both the COPA Commission report and the National Research Council report concluded that the government's interest in protecting children from harmful to minors material could be addressed through vigorous enforcement of other existing criminal statutes such as the Misleading Domain Name statute. P. Exh. 6, at 0046; P. Exh. 54, at 0136-0139.

685. More vigorous prosecution of the Misleading Domain Names statute would decrease the frequency with which minors inadvertently encounter unwanted sexually explicit material on the Internet. P. Exh. 6, at 0046; P. Exh. 54, at 0136-0139.

686. Defendant did not introduce any evidence at trial establishing that more vigorous enforcement of the Misleading Domain Names statute would not address the government's interest in protecting children from harmful to minors material.

2. Education: Encourage and Fund Educational Efforts.

687. Educating children about how to use the Internet safely is an effective method of ensuring their protection and safety online. Cranor Testimony, Oct. 24

Transcript, at 93:22-94:15; Taylor Testimony, Nov. 1 Transcript, at 167:2-7, 169:3-5; Kirk Testimony, Nov. 1 Transcript, at 79:24-83:15, 85:9-17; Smathers Testimony, Nov. 2 Transcript, at 14:22-15:1; P. Exh. 6, at 0018; P. Exh. 11, at 0022; P. Exh. 54, at 0253-0260, 0270-0273, 0284-0285.

688. Educating parents and teachers of minor children how to use the Internet safely, and to be aware of children's Internet usage, is an effective method of ensuring the safety of minors online. Cranor Testimony, Oct. 24 Transcript, at 93:22-94:15; Taylor Testimony, Nov. 1 Transcript, at 167:8-168:1; Kirk Testimony, Nov. 1 Transcript, at 71:1-13; Smathers Testimony, Nov. 2 Transcript, at 5:14-6:6.

689. The COPA Commission Report specifically found that family education programs are an essential part of an overall solution to protecting children online, and that because families are the first line of defense in protecting children, education programs can be highly effective in giving caregivers needed information about online risks and protection methods and access to technologies and ways to get help. The COPA Commission specifically recommended that the government, in combination with private industry, should undertake a major education campaign to promote public awareness of the various parental control tools. Cranor Testimony, Oct. 24 Transcript, at 95:7-96:3; P. Exh. 6, at 0018, 0040.

690. The National Research Council also concluded that the government's interest in protecting children from harmful to minors material could be addressed through increased education of parents and children about how to use the Internet safely. P. Exh. 54, at 0411-0413.

691. Congress could encourage additional educational efforts through pilot programs and funding. P. Exh. 6, at 0040-0041; P. Exh. 54, at 0411-0413.

692. Defendant did not introduce any evidence at trial establishing that increased educational efforts would not address the government's interest in protecting children from harmful to minors material.

3. Non-Technological Parental Control Tools: Fund and Encourage the use of Non-Technological Parental Control Tools.

693. Much like the non-content filtering software tools offered by filtering companies, such as the time management and monitoring technologies, there are a variety of non-technological parental control tools that can be valuable and effective measures in helping parents control their children's Internet activities. Cranor Testimony, Oct. 24 Transcript, at 92:1-13; P. Exh. 6, at 0033; P. Exh. 11, at 0020-24; P. Exh. 54, at 0246-85.

694. These non-technological parental control tools include placing the computer in a family room where its use can be observed, establishing ground rules for use of the Internet, actively monitoring the child's time on the computer, supervising and tracking the Web sites to which the child goes, and following "best practices" models for use of the Internet by children, such as discussing what is safe and not safe to do on the Internet, and what sorts of Web pages should and should not be accessed. Cranor Testimony, Oct. 24 Transcript, at 92:14-93:21; P. Exh. 6, at 0036; P. Exh. 11, at 0022-24; P. Exh. 54, at 0255-58.

695. These non-technological parental control tools are very helpful tools for parents to use to help control access to inappropriate material on the Internet. They are especially valuable because they engage the parent in the process, so that the parent can

understand what their children are doing on the Internet, and can interact with the children to explain what is appropriate and not appropriate to do online. Cranor Testimony, Oct. 24 Transcript, at 94:7-15, 99:13-25; P. Exh. 54, at 0246-48, 0287.

696. A number of studies have been conducted over the years that discuss the effectiveness of these non-technological tools. Those studies generally have concluded that non-technological parental control tools can be effective, especially when used in combination with the technological tools like filtering products. Cranor Testimony, Oct. 24 Transcript, at 94:21-95:6, 99:13-25. P. Exh. 6, at 18; P. Exh. 11, at 5; P. Exh. 54, at 0246-47, 0249.

697. A report from the Department of Commerce to Congress in August 2003 examined a number of these non-technological solutions. The report specifically found that the use of Internet safety policies, incorporating both technological and non-technological tools, can be effective at protecting children online, especially because of their flexibility and the fact that they can be customized to address the concerns of individual communities. The report noted that people who had implemented such safety policies had expressed a great deal of satisfaction regarding the effectiveness of those policies. Cranor Testimony, Oct. 24 Transcript, at 96:19-97:25; P. Exh. 11, at 5, 20-24, Appendix III.

698. Many parents are already utilizing these non-technological tools. According to a recent PEW Internet Research study, 73 percent of teenagers indicated that the household computer is placed in a public place in the home, and 64 percent of parents have set rules about their children's use of the Internet. Cranor Testimony, Oct. 24 Transcript, at 98:4-18; P. Exh. 85, at 45.

699. Congress could encourage the use of these non-technological parental control tools through pilot programs, through public relations efforts, and through funding. Cranor Testimony, Oct. 24 Transcript, at 99:5-12; P. Exh. 6, at 0040-42; P. Exh. 54, at 0261, 0272, 0282-85.

700. Defendant did not introduce any evidence at trial establishing that the increased use of these non-technological parental control tools would not address the government's interest in protecting children from harmful to minors material.

4. Congress Could Enact a More Limited, More Narrowly Tailored Statute.

a. The Statute Could Apply to Images Only.

701. COPA's prohibition on material that is harmful to minors applies to any "communication, picture, image, graphic image file, article, recording, writing, or other matter." COPA therefore applies to written material with no images, and to audio recordings and other materials with no images. 47 U.S.C. § 231(e)(6).

702. Congress could enact a statute that only applies to material containing harmful to minors images or pictures. Such a statute would be less restrictive than COPA.

703. Defendant did not introduce any evidence at trial establishing that a more limited statute that only applied to images would not address the government's interest in protecting children from harmful to minors material.

b. The Statute Could Impose Only Civil Penalties.

704. COPA imposes significant criminal penalties, including imprisonment, in addition to severe civil penalties for violation of the statute. 42 U.S.C. § 231(a)(1).

705. Congress could enact a statute that provides only for civil penalties, and does not subject Web sites to potential criminal liability. Such a statute would be less restrictive than COPA. P. Exh. 55, at 0003-0004.

706. Defendant opposed enactment of COPA on the ground that the government's interest in protecting children from harmful to minors material could be addressed through a more limited statute that only imposed civil penalties. P. Exh. 55, at 0003-0004.

707. The National Research Council report concluded that the government's interest in protecting children from harmful to minors material could be addressed through a more limited statute that only imposed civil penalties. P. Exh. 54.

708. Defendant did not introduce any evidence at trial establishing that a more limited statute that only imposed civil penalties would not address the government's interest in protecting children from harmful to minors material.

c. The Statute Could Require Labeling of Harmful to Minors Material.

709. COPA imposes severe criminal and civil penalties for distributing material that is harmful to minors over the Web. Congress could enact a statute that permits the distribution of such material, but instead requires Web site operators to include a rating, label, or other notification on the Web site that makes clear that harmful to minors material is available on the Web site. Such a rating, label or code could be placed on the initial home page of the site or in the hidden text, the metadata, associated with the site. Such a statute would be less restrictive than COPA. P. Exh. 6, at 0023; P. Exh. 54, at 0237.

710. A proposal to enact exactly this sort of statute has been endorsed by the current administration and has been introduced in Congress. The Department of Justice has issued public statements backing such a proposal as a means of protecting children. Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2006, H.R. 5749, 109th Cong. (2006); Project Safe Childhood Act, S. 3432, 109th Cong. (2006).

711. Such a statute would require end users to make a conscious, informed decision when they access harmful to minors content online, thus reducing the likelihood of inadvertent exposure to such content. P. Exh. 54, at 0236-0237.

712. Requiring Web sites to include a harmful to minors rating, label or notification would make filtering products even more effective and accurate at blocking harmful to minors material. P. Exh. 6, at 0042; P. Exh. 54, at 0310.

713. Both the COPA Commission report and the National Research Council report noted that the government's interest in protecting children from harmful to minors material could be addressed through a more limited statute that requires the rating or labeling of Web pages with harmful to minors material. P. Exh. 6, at 0042; P. Exh. 54, at 0310.

714. Defendant did not introduce any evidence at trial establishing that a more limited statute that required the rating or labeling of Web pages with harmful to minors material would not address the government's interest in protecting children from harmful to minors material.

d. The Statute Could Require Filtering Products to Contain a Harmful to Minors Category.

715. In a separate statutory provision not challenged here, Congress has required that ISPs and online service providers make information about parental control tools such as filtering products available to their customers. Congress could enact a statute that requires all companies or individuals distributing Internet content filtering products to include a harmful to minors category for parents to use to block material covered by COPA, and Congress could provide specific, express guidance as to what sorts of materials should be included in that category. Such a statute would be less restrictive than COPA.

716. Such a statute would enable companies that provide filtering products to block exactly the speech COPA seeks to prohibit.

717. Defendant did not introduce any evidence at trial establishing that a more limited statute that required all companies or individuals distributing Internet content filtering products to include a harmful to minors category in their products would not address the government's interest in protecting children from harmful to minors material.

e. Government-Provided List of Harmful to Minors Web Sites.

718. Congress could enact a statute requiring the Department of Justice or another governmental entity to compile and maintain a list of URLs that contain material that is harmful to minors. Alternatively, the Department of Justice could do so on its own initiative. Such a statute would be less restrictive than COPA. Allan Testimony, Nov. 2 Transcript, at 235:16-236:11, 236:15-21; Murphy Testimony, Nov. 1 Transcript, 99:9-100:22, 234:6-13, 235:18-20.

719. Such a statute would provide filtering product companies with the ability accurately to block absolutely all speech that the government believes is harmful to minors. Publication of the list would also provide parents and other entities with information about the types of material that are on the Web in order to assist parents in determining what protections, if any, are necessary for their children depending on their individual values and circumstances. Allan Testimony, Nov. 2 Transcript, at 235:16-236:11, 236:15-21; Murphy Testimony, Nov. 1 Transcript, 234:6-13, 235:18-20.

720. Filtering product companies could also be forced, by statute, to include a harmful to minor category in their products that contains all of the Web sites included on the government's list. The State of Utah recently passed a law requiring its Attorney General to compile an "adult content registry," a list of harmful to minors but non-obscene URLs. The law requires ISPs, at customer request, to block access to URLs on the adult content registry. H.B. 260, 2005 Gen Sess. of 56th Leg. (Utah 1999); Allan Testimony, Nov. 2 Transcript, at 235:16-236:11, 236:15-21; Murphy Testimony, Nov. 1 Transcript, 234:6-13; 235:18-20.

721. The filtering companies would be willing to review a governmentally-created list of inappropriate URLs, and add those URLS to their blacklists, or place them in categories deemed inappropriate for minors. Allan Testimony, Nov. 2 Transcript, at 235:16-236:21; Murphy Testimony, Nov. 1 Transcript, at 234:18-235:20.

722. Defendant did not introduce any evidence at trial establishing that a more limited statute that required the Department of Justice or another governmental entity to compile and maintain a list of URLs that contain material that is harmful to minors

would not address the government's interest in protecting children from harmful to minors material.

f. Funding of an Independent Rating System.

723. Congress could fund an independent organization to rate Web sites and make such ratings available to parents for their use. P. Exh. 6, at 0023-25, 0033; P. Exh. 54, at 0355-67.

724. Such a rating system would make filtering products even more effective and accurate at blocking materials that are harmful to minors. P. Exh. 54, at 0355-58.

725. The National Research Council report concluded that the government's interest in protecting children from harmful to minors material could be addressed through the funding of an independent Web site rating system. P. Exh. 54, at 0355-58.

726. The COPA Commission report similarly concluded that independent rating of Web sites could be an effective measure to address the government's interest in protecting children from harmful to minors material. P. Exh. 6, at 24.

727. Defendant did not introduce any evidence at trial establishing that the funding of an independent rating system would not address the government's interest in protecting children from harmful to minors material.

g. Government-Provided List of Parental Control Resources.

728. Congress could enact a statute requiring the creation and maintenance of a government-provided list of online parental control resources. P. Exh. 6, at 17.

729. Such a statute would provide parents with the information and resources necessary to make informed and educated decisions about the best ways for them to protect their children on the Internet, based on their individual values and desires. P. Exh. 6, at 17.

730. Online information resources are essential to protecting children on the Internet, and provide substantial benefits to parents seeking to protect their children. P. Exh. 6, at 17.

731. Defendant did not introduce any evidence at trial establishing that the creation of a government-provided list of online parental control resources would not address the government's interest in protecting children from harmful to minors material.

h. Government-Testing of Filtering Products.

732. Congress could enact a statute requiring a federal agency or department to conduct testing of the various filtering products available for parents to use, and to publish and publicize that testing. P. Exh. 6, at 41.

733. Such a statute would provide parents with the information and resources necessary to make informed and educated decisions about which filtering products, if any, are best for them to use to protect their children on the Internet, based on their individual values and desires. P. Exh. 6, at 41.

734. The COPA Commission report specifically recommended that the government allocate resources for the independent evaluation of child protection technologies and to provide reports about such evaluations to the public. P. Exh. 6, at 41.

735. Defendant did not introduce any evidence at trial establishing that government testing of filtering products and the publication of those test results would not address the government's interest in protecting children from harmful to minors material.

CONCLUSIONS OF LAW

In addition to the following Conclusions of Law, Plaintiffs respectfully direct the Court's attention to their Trial Memorandum, which elaborates on many of the legal points set out briefly below.

1. Once a court determines that one of the Plaintiffs has standing, it need not decide the standing of the other Plaintiffs. Article III limits the jurisdiction of the federal courts to justiciable cases or controversies. U.S. Const., Art. III, § 2. The "presence of one party with standing assures that controversy before [the] Court is justiciable." *Dep't of Commerce v. U.S. House of Representatives*, 525 U.S. 316, 330 (1999) (internal citation omitted).

2. In a First Amendment facial challenge to a statute, a credible threat of present or future criminal prosecution is sufficient to confer standing. *See Va. v. Am. Booksellers Ass'n*, 484 U.S. 383, 392 (1988); *ACLU v. Reno*, 31 F. Supp. 2d 473, 479 (E.D. Pa. 1999).

3. COPA applies to those who, "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, make[] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors. . . ." 47 U.S.C. § 231(a)(1)-(3).

4. COPA defines "commercial purposes" as being "engaged in the business of making such communications." 47 U.S.C. § 231(e)(2)(A). COPA then defines "engaged in the business" as meaning:

> [T]hat the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a

> profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income).
>
> 47 U.S.C. § 231(e)(2)(B).

5. COPA's definition of the term "commercial purposes" is so broad that it encompasses many Web site operators who provide their speech for free. *ACLU v. Ashcroft*, 322 F.3d 240, 256-57 (3d Cir. 2003) (stating that the "'engaged in the business' definition would encompass . . . the Web publisher who provides free content on his or her Web site and seeks advertising revenue, perhaps only to defray the cost of maintaining the Web site").

6. COPA's definition of the term "commercial purposes" demonstrates that COPA is not limited in its application to "commercial pornography." *See ACLU v. Ashcroft*, 322 F.3d 240, 256 (3d Cir. 2003) ("There is nothing in the text of COPA . . . that limits its applicability to so-called commercial pornographers only.") (*quoting ACLU v. Reno*, 31. F. Supp.2d 473, 480 (E.D. Pa. 1999)).

7. COPA defines "minor" as "any person under 17 years of age." 47 U.S.C. § 231(e)(7). COPA is not narrowly targeted at content that is harmful to "older" minors, but rather applies to all minors. *ACLU v. Ashcroft*, 322 F.3d at 240, 253-55 (3d Cir. 2003).

8. COPA defines materials that are "harmful to minors" as follows:

> any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that -- (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd

> exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.
>
> 47 U.S.C. § 231(e)(6).

9. COPA's definition of "harmful to minors" refers to material that "as a whole," appeals or panders to the prurient interest of minors. 47 U.S.C. § 231(e)(6)(A). Properly read, "as a whole" applies to "each individual communication, picture, image, exhibit, etc." *ACLU v. Ashcroft*, 322 F.3d 240, 252 (3d Cir. 2003).

10. COPA's definition of "harmful to minors" refers to "contemporary community standards." 47 U.S.C. § 231(e)(6)(A). The consequence of COPA's incorporation of community standards is that "the statute effectively limits the range of permissible material under the statute to that which is deemed acceptable only by the most puritanical communities." *Ashcroft v. ACLU*, 322 F.3d 240, 252 (3d Cir. 2003).

11. COPA applies to communications in "interstate or foreign commerce by means of the World Wide Web." 47 U.S.C. § 231 (2006). This language, and COPA's legislative history, do not support extraterritorial application.

12. Statutes are presumed to have domestic effect only, unless an analysis of the statutory language and the legislative history illustrate a clear, unambiguous congressional intent to legislate beyond U.S. borders. This presumption against extraterritorial application applies to statutes that provide for both civil and misdemeanor criminal penalties, such as COPA. *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949).

13. COPA's phrasing is insufficient to demonstrate Congress' clear and unambiguous intent that COPA applies to Web sites that are hosted or registered outside the United States. *See, e.g.*, *N.Y. Cent. R.R. Co. v. Chisholm*, 268 U.S. 29, 31-32 (1925)

(applying the presumption against extraterritoriality to defeat extraterritorial application for a statute regulating "interstate or foreign commerce"); *United States v. Reeves*, 62 M.J. 88 (C.A.A.F. 2005) (applying the presumption against extraterritoriality to a statute that prohibited conduct "in interstate or foreign commerce").

14. If Congress had intended for COPA to have extraterritorial application, it could have inserted appropriate language in the statute. *See, e.g.*, Maritime Drug Law Enforcement Act, 46 U.S.C. app. § 1903(h) (2006) ("This section is intended to reach acts… outside the territorial jurisdiction of the United States.").

15. The legislative history also does not support a finding that Congress intended for COPA to apply to Web sites that are hosted or registered outside the United States. *See*, *e.g.*, H.R. REP. NO. 105-775, pt. III (1998) ("Clearly domestic restrictions in the United States will help reduce a child's access to pornography, and it may even help protect children in foreign nations who are the recipients of this burgeoning export trade. To the extent that an international problem exists, the Committee has requested that the Commission on Online Child Protection study the matter and report back to Congress.") (internal quotation marks omitted).

16. Enforcement of COPA against overseas websites is burdensome and impractical. The exercise of specific jurisdiction is dependent on a sliding scale of commercial interactivity for the Web site in question. Merely posting something on the Internet that is accessible to users in foreign jurisdictions, known as a "passive site," is not grounds for jurisdiction to attach. *Zippo Mfg. Co. v. Zippo Dot Com. Inc.*, 952 F. Supp. 1119, 1121 (W.D. Pa. 1997); *Toys "R" Us, Inc. v. Step Two, S.A.*, 318 F.3d 446, 452 (3d Cir. 2003); *Barrett v. Catacombs Press*, 44 F. Supp. 2d 717 (E.D. Pa. 1999).

17. Even if a court ultimately finds it has personal jurisdiction over an overseas Web site, there is no method to ensure that the Web site obeys the judgment of the U.S. court. *See, e.g.*, *Phillip Morris USA, Inc. v. Otamedia Ltd.*, 331 F. Supp. 2d 228 (S.D.N.Y. 2004) (overseas Web site selling Phillip Morris cigarettes continued to sell product even after court entered judgment against them).

18. COPA is a content-based regulation. Specifically, it regulates speech with "harmful to minors" content. 47 U.S.C. § 231(a).

19. Content-based regulations are subject to strict scrutiny. *See Turner Broadcasting Sys., Inc. v. F.C.C.*, 512 U.S. 622, 642 (1994). Such regulations are presumptively invalid. *See R.A.V. v. City of St. Paul*, 505 U.S. 377, 391 (1992).

20. COPA proscribes large quantities of speech that is constitutionally protected for adults. *See ACLU v. Ashcroft*, 322 F.3d 240, 252 (3d Cir. 2003) ("Because COPA's definition of harmful material is explicitly focused on minors, it automatically impacts non-obscene, sexually suggestive speech that is otherwise protected for adults.").

21. Statutes may not suppress an unnecessarily broad quantity of speech protected for adults in the name of protecting minors. *Reno v.* ACLU, 521 U.S. 844, 875 (1997) (citations omitted) ("[T]he governmental interest in protecting children from harmful materials . . . does not justify an unnecessarily broad suppression of speech addressed to adults.").

22. Under strict scrutiny, regulations are upheld only where the defendant, who shoulders the burden of proof, demonstrates that they are justified by a compelling governmental interest, "narrowly tailored" to effectuate that interest, and the least

restrictive means of advancing that interest. *ACLU v. Ashcroft*, 322 F.3d 240, 251 (3d Cir. 2003).

23. Laws are not narrowly tailored where they are overinclusive. Overinclusive laws prohibit a substantial amount of speech the suppression of which does not advance the government's compelling interest. *See Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.*, 502 U.S. 105, 121 (1991).

24. The affirmative defenses cannot cure COPA's overinclusiveness because they will deter listeners, many of whom will be unwilling to reveal personal information in order to access content. *See Denver Area Educational Telecommunications Consortium, Inc. v FCC*, 518 U.S. 727, 754 (1996) (striking down an identification requirement because it would "further restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the 'patently offensive' channel.").

25. The affirmative defenses cannot cure COPA's overinclusiveness because they are effectively unavailable. Credit cards, debit accounts, adult access codes, and adult personal identification numbers do not verify age. As a result, their use does not, "in good faith," "restrict[] access" by minors. 47 U.S.C. § 231(c)(1)(A).

26. Requiring use of the affirmative defenses places an impermissible economic burden on the exercise of protected speech because all of them involve considerable cost. *See Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.,* 502 U.S. 105, 115 (1991) ("A statute is presumptively inconsistent with the First Amendment if it imposes a financial burden on speakers because of the content of their speech.").

27. Requiring use of the affirmative defenses impermissibly burdens speech because it subjects Web speakers to the hecklers' veto. *See Reno v. ACLU*, 521 U.S. 844, 880 (1997).

28. The affirmative defenses impermissibly burden Web site operators with demonstrating that their speech is lawful. *See Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 255 (2002) ("The Government raises serious constitutional difficulties by seeking to impose on the defendant the burden of proving his speech is not unlawful."); *Ashcroft v. ACLU*, 322 F.3d 240, 260 (3d Cir. 2003) (noting that "the affirmative defenses do not provide the Web publishers with assurances of freedom from prosecution.").

29. Because the affirmative defenses make it difficult for speakers in the United States to communicate with those overseas, requiring their use infringes the First Amendment right of Web site operators to communicate with foreign audiences. *Bullfrog Films, Inc. v. Wick,* 847 F.2d 502, 509 n.9 (9th Cir. 1998).

30. Laws are not narrowly tailored where they are underinclusive. Underinclusive laws like COPA fail to restrict a substantial amount of speech that harms the government's compelling interest. *See Florida Star v. B.J.F.*, 491 U.S. 524, 540 (1989); *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n,* 447 U.S. 557, 564 (1980).

31. Payment card associations, payment card issuers, acquiring banks, payment card intermediaries, mobile carriers, and Internet Service Providers are not required to enforce COPA against Web sites, domestic or outside the U.S., that provide content that is harmful to minors. *See* 47 U.S.C. § 231.

32. Content-based speech restrictions must be held unconstitutional where the government fails to prove that they are the least restrictive means of serving the stated governmental interest. *See Ashcroft v. ACLU*, 542 U.S. 656, 665 (2004) ("When plaintiffs challenge a content-based speech restriction, the burden is on the Government to prove that the proposed alternatives will not be as effective as the challenged statute.").

33. "Blocking and filtering software is an alternative that is less restrictive than COPA." *Ashcroft v. ACLU,* 542 U.S. 656, 666-67 (2004).

34. The Supreme Court expressly rejected defendant's argument that filters are not a less restrictive alternative because they are part of the status quo. The Court held that filtering software is an eligible less restrictive alternative because government could "act to encourage the use of filters" and could "take steps to promote their development by industry, and their use by parents." *Ashcroft v. ACLU*, 542 U.S. 656, 669-70 (2004).

35. Given "Congress' goal of shielding minors from pornographic teasers," COPA could have prohibited "only pictures, images, or graphic image files, which are typically employed by adult entertainment Web sites as 'teasers.'" *ACLU v. Reno*, 31 F. Supp.2d 473, 497 (E.D. Pa. 1999).

36. For the reasons stated above, COPA also violates the First Amendment because it is overbroad. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 244 (2002) ("The overbreadth doctrine prohibits the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process.").

37. The Court must scrutinize COPA's terms for vagueness especially closely because it is a content based speech regulation that imposes criminal penalties. *See ACLU v. Reno*, 521 U.S. 844, 871-72 (1997).

38. The phrase "considered as a whole" is vague when applied to the Web, where there is no logical way for a speaker to define the relevant "whole" when trying to determine the legality of a Web site comprised of thousands of linked documents, images, and texts, simultaneously presented through the ad hoc linking feature of the Web.

39. The term "minors" is vague as used in COPA because it is unclear what the dispositive minimum age is for determining whether content is "harmful." *ACLU v. Ashcroft*, 322 F.3d 240, 268 n.37 (3d Cir. 2003) ("The fearful Web publisher therefore will be forced to assume, and conform his conduct to, the youngest minor to whom the statute conceivably could apply. We cannot say whether such a minor would be five years of age, three years, or even two months.")

40. While COPA imposes severe additional penalties for "intentional" as opposed to "knowing" violations, it fails to define the distinction between the two requisite levels of knowledge for prosecution. *See* 47 U.S.C. § 231(a)(1)-(2).

41. COPA's affirmative defenses interfere with the First Amendment right to access information anonymously because they require the disclosure of personally identifying information. 47 U.S.C. § 231(c); *Bd. of Educ. v. Pico,* 457 U.S. 853, 866-67 (1982) ("[T]he First Amendment protects the right to receive information and ideas."); *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965) (invalidating statute requiring that individuals request certain mail in writing on grounds of "deterrent effect").

42. The right of anonymous communication has enjoyed judicial protection in a variety of settings, including the Internet. *See, e.g.*, *McIntyre v. Bd. of Elections Comm'n,* 514 U.S. 334 (1995) (striking down Ohio statute prohibiting anonymous distribution of campaign literature); *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) ("[T]he constitutional rights of Internet users, including the right to speak anonymously, must be carefully safeguarded").

43. COPA conditions receiving Web content on the loss of anonymity and impermissibly deters adults who fear stigma and exposure from communicating and receiving non-obscene information. *See ACLU v. Johnson*, 4 F. Supp.2d 1029, 1033 (D. N.M. 1998) (emphasis added) (striking down New Mexico's online harmful-to-minors law, and holding that the act "violate[d] the First and Fourteenth Amendments of the United States Constitution because it prevent[ed] people from communicating *and* accessing information anonymously.").

44. COPA does not provide any recourse to users for confidentiality violations by Web sites. In fact, COPA explicitly grants immunity to content providers for any action taken to comply with COPA. 47 U.S.C. § 231(c)(2).

45. COPA's statutory protections against wider disclosure of personal information are insufficient in themselves to cure the constitutional defect. The protections guard only against *additional* disclosures of identifying information; in order to gain access to Web sites, however, users will *already* have been required to disclose their identities to Web site operators, thereby breaching their anonymity. 47 U.S.C. § 231(d). *See ACLU v. Reno*, 31 F. Supp. 2d 473, 485 (E.D. Pa. 1999) (noting testimony that "the internet is a valuable resource for 'closeted' people who do not voluntarily disclose their sexual

orientation due to fear of the reactions of others because it allows closeted people to access this information while preserving their anonymity.").

46. COPA's prohibition on additional disclosure is ineffective because it imposes no penalties on those who violate its disclosure provisions. *ACLU v. Ashcroft*, 322 F.3d 240, 259 n.21 (3d Cir. 2003) (discounting COPA's prohibition on disclosure because COPA does not impose penalties on Web site operators who violate its provisions); *Denver Area,* 518 U.S. at 754 (noting that disclosure provisions "will further restrict" communication by people "who fear for their reputations should the operator, *advertently or inadvertently*, disclose the list of those who wish to watch the 'patently offensive' channel.") (emphasis added).

47. Older minors enjoy robust First Amendment protections. *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-13 (1975) (citations omitted) ("[M]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them.").

48. This right extends to material that is sexually explicit. *ACLU v. Reno,* 929 F. Supp. 824, 852 (E.D. Pa. 1996) (stating that "at least some of the material subject to coverage under the 'indecent' and 'patently offensive' provisions of the CDA may contain valuable literary, artistic or educational information of value to older minors as well as adults.").

49. COPA prohibits minors from viewing material the government deems "harmful to minors" even where parents wish their children to have access to such

material. *Reno v. ACLU*, 521 U.S. 844, 845 (1997) (striking down the Communications Decency Act in part because it included no parental override).

50. Courts have struck down numerous laws that prohibited "harmful to minors" content on the Internet. *Am. Booksellers Found. for Free Expression v. Dean*, 202 F. Supp.2d 300 (D. Vt. 2002), aff'd in pertinent part, 342 F.3d 96 (2d Cir. 2003) (enjoining the enforcement of a Vermont "harmful to minors" law applied to Internet communications); *Cyberspace Comm., Inc. v. Engler*, 55 F. Supp.2d 737 (E.D. Mich. 1999), *aff'd* 238 F.3d 420 (6th Cir. 2000), *summary judgment granted*, 142 F. Supp.2d 827 (E.D. Mich. 2001) (enjoining a Michican "harmful to minors" law applied to Internet communications); *Bookfriends, Inc. v. Taft*, 223 F. Supp.2d 932 (S.D. Ohio 2002) (enjoining an Ohio "harmful to juveniles" law applied to Internet communications); *ACLU v. Johnson*, 194 F. 3d 1149 (10th Cir. 1999); PSINet*, Inc. v. Chapman*, 167 F. Supp.2d 878 (W.D. Va. 2001), *aff'd* 362 F.3d 227 (4th Cir. 2004) (enjoining a Virginia "harmful to minors" law that was applied to Internet communications); *Southeast Booksellers v. McMasters*, 282 F. Supp2d 1180 (D.S.C. 2003) (enjoining the enforcement of a South Carolina "harmful to minors" law that was applied to Internet communications); *Am. Library Assoc. v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997).

December 8, 2006

Respectfully submitted,

/s/

Christopher A. Hansen
Aden Fine
Benjamin Wizner
Catherine Crump
American Civil Liberties Union

125 Broad Street – 18th floor
New York, NY 10004
(212) 549-2693

_____/s/_____
Christopher Harris
Seth Friedman
Katharine Marshall
Jeroen van Kwawegen
Elan R. Dobbs
Latham & Watkins LLP
885 Third Avenue
New York, NY 10022
(212) 906-1800

For Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on December 8, 2006, I electronically filed Plaintiffs' Post-Trial Proposed Findings of Fact and Conclusions of Law with the Clerk of the Court using the ECF system, which will send notification of such filing to Raphael O. Gomez, Department of Justice.

/s/

Catherine Crump
American Civil Liberties Union
125 Broad Street – 18th floor
New York, NY 10004
Counsel for Plaintiffs